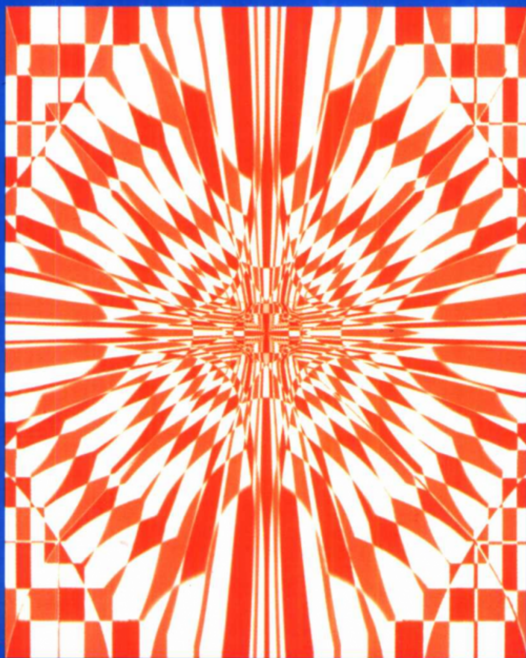
北京大学数学丛书

数论及其应用

李文卿 著



北京大学出版社

北京大学数学丛书

数论及其应用

李文卿 著

北京大学出版社

·北 京·

图书在版编目(CIP)数据

数论及其应用/李文卿著. —北京：北京大学出版社，2001.3
(北京大学数学丛书/程民德主编)
ISBN 7-301-04169-1

Ⅰ. 数…　Ⅱ. 李…　Ⅲ. 数论　Ⅳ. O156

中国版本图书馆 CIP 数据核字(1999)第 17241 号

书　　名：数论及其应用
著作责任者：李文卿
责 任 编 辑：邱淑清
标 准 书 号：ISBN 7-301-04169-1/O · 445
出　版　者：北京大学出版社
地　　址：北京市海淀区中关村北京大学校内　100871
网　　址：http://cbs.pku.edu.cn/cbs.htm
电　　话：出版部 62752015　发行部 62754140　理科编辑部 62752021
电 子 信 箱：zpup@pup.pku.edu.cn
排　版　者：北京大学印刷厂
印　刷　者：北京大学印刷厂
发　行　者：北京大学出版社
经　销　者：新华书店
850 毫米×1168 毫米　32 开本　12.25 印张　302 千字
2001 年 3 月第一版　　2001 年 3 月第一次印刷
定　　价：20.00 元

前　言

在过去的 10 年中，通过精确构造所谓的 Ramanujan 图，数论在网络通讯及计算复杂性方面有了非常重要的应用. Ramanujan 图是一些其非平凡特征值都很小的正则图 (详细说明参见本书的第九章). 到目前为止, 所有已知的 Ramanujan 图的构造都源于数论: 一种想法基于模形式的 Fourier 系数的估计，即由 Deligne 证明的 Ramanujan-Petersson 猜想；另一种想法则依赖于一些特征和的估计，这些估计可由被 Weil 证明的有限域上的代数曲线的 Riemann 猜想导出. 这两种思路的共同背景是著名的 Weil 猜想，该猜想已在 1973 年被 Deligne 所证明. 这即是我们这本书的出发点. 本书的目的是介绍与上述应用相关的数论知识，最终给出 Ramanujan 图的精确构造. 事实上, 我们希望通过以这样一个简单的目标作为本书取材和论述的基础，让读者能够接触到现代数论里一些最深奥、最精美的部分.

这是一本为高年级本科生，研究生和对数论及其应用感兴趣的人写的书. 其风格是半正式的. 作者假定读者已经有了一些代数及数论的基础知识. 在此基础上，作者尽可能地保持本书的自封性. 我们的主要目的是介绍相关的基本概念和结果, 同时也给出一些难度较大的定理的证明提要，以便让读者能比较完整地了解所阐述的理论体系和思想方法. 一般地, 没有给出证明的论述都可以假定成立, 而不影响论述的完整性. 有兴趣的读者可以从每章后的参考文献里找到所有省略的材料以及没有讨论的相关的内容. 贯穿本书，我们准备了许多习题，以便让读者有机会练习，其中，有些习题将用于定理的证明.

全书的内容安排如下：在第一章复习了有限域的基本概念之后，第二章将讨论关于有限域上 zeta 函数的 Weil 猜想. 我们将

看到 Weil 是如何从计算一个多项式方程在有限域的扩张上的解的个数来导出他的这一著名猜想的. 同时, 我们将介绍证明这一猜想的思想方法. 第三章研究和讨论局部域与整体域. 在本书中, 我们将用阿代尔语言来描述整体域. 第四和第五章是关于函数域的, 其中, 我们将证明 Riemann-Roch 定理, 并介绍结合伊代尔类特征标的 L-函数和 zeta 函数的解析性质. 借助于类域论的一些结果 (书中我们将给出简单的概述), 并结合第五章和第二章中讨论的 L-函数和有限域上曲线的 Riemann 猜想, 我们在第六章将给出一些特征和的估计, 这些估计将用于第九章中的 Ramanujan 图的构造. 第七章讨论经典模形式, 这是一个内容非常丰富且与数学的许多分支都有深刻联系的理论. 我们将概述该理论的发展, 包括 Hecke 算子、 L-函数、模形式逆定理, 以及新形式理论. 我们还将讨论这一领域中的主猜想及其推论, 其中有些推论在数论中有着极其深远的影响, 例如椭圆曲线理论中的 Taniyama-Shimura 猜想, 最近 Wiles 以及 Taylor 和 Wiles 的工作证明它关于半稳定的椭圆曲线是正确的, 这一结果结合早先 Frey 和 Ribet 的结果即可肯定著名的 Fermat 大定理是正确的. 自守形式和自守表示将在第八章讨论, 在这一章中, 我们先用阿代尔语言重新刻画模形式, 由此自然导出 GL(2) 上的自守形式和自守表示的概念. 接下来论述 Jacquet-Langlands 关于 GL(2) 和四元数群上局部表示和整体表示的理论. 特别地, 我们将描述这些群的局部表示是如何被其结合的 L-因子和 ε-因子决定的, 由此得到这些群的局部表示之间的关系. 最后, 我们将在第九章看到数论与组合学的联系. 一方面我们利用前面的讨论给出 Ramanujan 图的精确构造, 另一方面, 通过研究一些由四元数群产生的图的测度的极限, 我们可以得到有关 Hecke 算子的特征值分布的一些结果.

这本书源于作者于 1992 至 1993 年在台湾大学讲授的为期一年的研究生数论课程. 在此之前, 作者曾用该书的基本素材于 1992 年夏在四川大学由国家教委举办的研究生数学夏令营作了一个月

的讲座. 作者非常感谢这两所大学的支持和协助. 听众的热情也给予作者极大的鼓励. 本书的主要部分是作者在 1992 至 1993 年在台湾大学访问时完成的. 我特别要感谢台湾国家科学委员会和美国 National Security Agency 的财政支持, 以及王绣丽女士出色的打字工作. 本书最后是在 1995 年春在作者访问 Berkeley 数学科学研究所时完成的. 在此我也要向该所所给予的热情接待和支持表示由衷的谢意.

本书的原稿是用英文写成的, 中文稿是由中国科技大学李云峰先生翻译整理的. 第七章之后的附录是他写的, 有些习题也是他加的. 对李先生的热心协助及细心编排、翻译和校对, 作者在此表示由衷的谢意. 要是没有他的积极推动, 本书极可能无法与读者见面. 另外, 我还要感谢丁石孙先生的建议, 将本书译成中文, 由北大出版社出版. 作者衷心地希望国内喜爱数论的人士或能从该书中略窥数论之奥秘与精深.

李文卿

1995 年春于加州 Berkeley 数学科学研究所

目 录

第一章　有　限　域

§1　有限域的结构

顾名思义，**有限域**就是只有有限个元素的域. 最简单的例子是素域 $F_p = \mathbf{Z}/p\mathbf{Z}$, 其中 p 为素数.

设 F 是一个域，映射

$$\begin{aligned}\varphi : \mathbf{Z} &\longrightarrow F\\ n &\longmapsto n\cdot 1 = 1+1+\cdots+1(n\ 次)\end{aligned}$$

的像是整环，从而同构于 $\mathbf{Z}$ 或 $\mathbf{Z}/p\mathbf{Z}$, 其中 p 为素数. 对于前者，称 F 为 **特征**
rm 0 域; 对于后者，称 F 为 **特征 p 域**. F 的特征记作 $\mathrm{char}(F)$. 如果 $\mathrm{char}(F) = p \neq 0$, 那么 p 也是满足 $n\cdot 1 = 0$ 的最小自然数 n.

习题 1　设 F 是一特征 p 域，则对任意自然数 d 有

$$(x+y)^{p^d} = x^{p^d} + y^{p^d}, \qquad x, y \in F.$$

有限域的特征明显是不为 0 的；但反过来，特征不为 0 的域并不一定是有限域. 请有兴趣的读者构造特征 0 的无限域.

设 k 是一有限域， $\mathrm{char}(k) = p$, 则它包含 $\mathbf{Z}/p\mathbf{Z}$ 作为它的一个子域，进而是 $\mathbf{Z}/p\mathbf{Z}$ 上的一个有限维向量空间，因此它的势 $|k| = q = p^d$ 是 p 的幂，其中指数 d 是向量空间 k 在 $\mathbf{Z}/p\mathbf{Z}$ 上的维数. 这也导出 k 的加法群是 d 个的 p 阶循环群的直和.

下面考虑乘法群 $k^{\times} = k \setminus \{0\}$, 它的阶是 $q-1$. 于是 k 中任何非 0 元素均满足

$$x^{q-1} = 1.$$

进而 $k^\times$ 中元素的阶整除 $q-1$. 对 $q-1$ 的每个正因子 r, 设

$$\Omega(r)=\{x\in k^\times : x \text{ 的阶是 } r\}.$$

则随着 r 跑遍 $q-1$ 的所有正因子, $k^\times$ 是这些 $\Omega(r)$ 的非交并. 我们希望证明 $\Omega(q-1)$ 是非空的, 即

定理 1 *$k^\times$ 是 $q-1$ 阶循环群.*

为证此定理, 我们先证一个如下的一般的事实.

引理 1 *域 F 上的一个 n 次多项式在 F 中至多有 n 个不同的根.*

证 设 $f(x)\in F[x]$, α 为 $f(x)$ 在 F 中的一个根, 则 $f(\alpha)=0$. 于是

$$f(x)=f(x)-f(\alpha)=(x-\alpha)g(x),$$

这里 $g(x)$ 为 F 上 $n-1$ 次多项式. 若 β 为 $f(x)$ 在 F 中的一个不同于 α 的根, 则可由

$$0=f(\beta)=(\beta-\alpha)g(\beta)$$

和 $\alpha\neq\beta$ 导出 $g(\beta)=0$. 利用归纳法, $n=1$ 时引理显然成立. 假设 $n-1$ 时引理成立, 则 $g(x)$ 在 F 中至多有 $n-1$ 个不同的根. 于是 $f(x)$ 在 F 中至多有 n 个不同的根. 由此引理得证.

由引理 1 可知, 若 $\Omega(r)$ 是非空的, 设它包含有元素 y, 则 y 生成一个 r 阶循环子群 $\langle y\rangle$, 它由所有 $x^r=1$ 在 k 中的解组成. $\Omega(r)$ 为循环群 $\langle y\rangle$ 的生成元集, 即

$$\Omega(r)=\{y^i : 1\le i\le r, \gcd(i,r)=1\}.$$

这就证明了 $\Omega(r)$ 的势或者为 0 或者为 $\phi(r)$. 这里 $\phi(n)$ 是 Euler ϕ 函数, 它表示在 1 到 n 之间与 n 互素的整数的个数. 从而

$$|k^\times|=q-1=\sum_{r|q-1}|\Omega(r)|\le\sum_{r|q-1}\phi(r).$$

在初等数论中有如下一个结论.

引理 2 对自然数 m, $\sum_{r|m}\phi(r)=m$.

我们立刻由此引理及其上面的不等式得出：对任意的 $r|q-1$ 均有 $|\Omega(r)|=\phi(r)$. 特别地，$|\Omega(q-1)|=\phi(q-1)\geq 1$. 由此，定理 1 得证.

为证引理 2, 我们将 $\{1,2,\cdots,m\}$ 分拆成下面类型集合的不交并

$$Y(r)=\left\{1\leq i\leq m:\gcd(i,m)=\frac{m}{r}\right\},$$

这里 r 跑遍 m 的所有正因子. 对 $i\in Y(r)$, 记 $i=j\frac{m}{r}$, 则 $1\leq j\leq r$ 且 $\gcd(j,r)=1$. 因此 $|Y(r)|=\phi(r)$, 由此就可导出引理 2.

上述讨论有下面一些推论.

推论 1 在 $\mathbf{Z}/p\mathbf{Z}$ 的一个包含 k 的代数闭包中，域 k 由方程 $x^q-x=0$ 的解组成.

推论 2 存在 k 中元素 ξ, 使得 $k=(\mathbf{Z}/p\mathbf{Z})(\xi)$, 即 k 是素域 $\mathbf{Z}/p\mathbf{Z}$ 的一个单扩张.

推论 3 对 $q-1$ 的每个正因子 r, 在 $k^\times$ 中恰好存在 $\phi(r)$ 个元素，其阶为 r.

推论 4 给出一个正整数 n, 在 $\mathbf{Z}/p\mathbf{Z}$ 的一个代数闭包中，唯一存在一个 $\mathbf{Z}/p\mathbf{Z}$ 的 n 次域扩张.

证 推论 1 表明：如果存在一个 $\mathbf{Z}/p\mathbf{Z}$ 在其代数闭包中的 n 次扩张，那么该扩张恰由 $x^{p^n}=x$ 的根所组成. 另一方面，容易验证：若 α,β 为 $x^{p^n}=x$ 的解，则 $\alpha-\beta$ 和 $\alpha\beta^{-1}(\beta\neq 0)$ 也是 $x^{p^n}=x$ 的解. 故 $x^{p^n}=x$ 的解构成一个域. 因此推论得证.

推论 5 任给自然数 n, 存在 $\mathbf{Z}/p\mathbf{Z}$ 上的 n 次不可约多项式.

证 设 k 为 $\mathbf{Z}/p\mathbf{Z}$ 上的 n 次扩张. 由推论 2 知，存在 ξ 使得 $k=(\mathbf{Z}/p\mathbf{Z})(\xi)$. 设 $f(x)$ 为 ξ 在 $\mathbf{Z}/p\mathbf{Z}$ 上的不可约多项式，则由

$$k=(\mathbf{Z}/p\mathbf{Z})(\xi)=(\mathbf{Z}/p\mathbf{Z})[\xi]\cong(\mathbf{Z}/p\mathbf{Z})[x]/(f(x))$$

可得 $\deg f = [k : \mathbf{Z}/p\mathbf{Z}] = n$.

§2 有限域的扩张

在本节中，设 k 是一个有 q 个元素的有限域，k_n 为 k 的 n 次域扩张．k_n 的任意包含 k 的子域必为 k 的有限扩张；若其扩张次数为 m, 则 m 可整除 n. 反过来，由推论 1 可知，对 n 的任意正因子 m, 在 k_n 的一个代数闭包中，k 的 m 次扩张均为 k_n 的子域.

习题 2 上述论述中用到了这样一个事实："设 F 为一个有限域，它有一个势为 q 的子域 K, 则 F 的势为 q^n, 其中 n 是 F 在 K 上的扩张次数 $[F : K]$." 试证明此结论成立.

对域 F 的一个扩张 E, 以 $\mathrm{Gal}(E/F)$ 表示 E 的所有使 F 不变的自同构集合，它构成一个群 (请读者自己验证). 注意到 $\mathrm{Gal}(E/F)$ 中元素可视为 E 上的 F 线性变换．进一步，我们有如下结果.

引理 3 $\mathrm{Gal}(E/F)$ *中的自同构是 E 线性无关的.*

证 假设引理不真，则可列出一长度最短的非平凡的线性关系

$$a_1\tau_1 + \cdots + a_r\tau_r = 0$$
$$(a_i \in E^{\times}, \tau_i \in \mathrm{Gal}(E/F),\quad i = 1, \cdots, r). \tag{2.1}$$

必然有 $r \geq 2$, 且 τ_i 都是互不相同的．因为 $\tau_1 \neq \tau_2$, 所以存在元素 $y \in E$, 使得 $\tau_1(y) \neq \tau_2(y)$. 由 (2.1) 式得出另一关系：对任意的 $x \in E$, 有

$$0 = \sum_{i=1}^{r} a_i\tau_i(yx) = \sum_{i=1}^{r} a_i\tau_i(y)\tau_i(x),$$

从而 $\sum\limits_{i=1}^{r} a_i\tau_i(y)\tau_i = 0$. 这就导出第三个非平凡的线性关系：

$$0 = \sum_{i=1}^{r} a_i\tau_i(y)\tau_i - \tau_1(y)\sum_{i=1}^{r} a_i\tau_i = \sum_{i=2}^{r}(\tau_i(y) - \tau_1(y))\tau_i,$$

其长度比前述关系 (2.1) 要短，这与 (2.1) 式的选取相矛盾.

引理 4 设 E 为域 F 的 n 次扩张, 则在 $\mathrm{Gal}(E/F)$ 中至多有 n 个不同的自同构.

证 假设引理不真, 则 $\mathrm{Gal}(E/F)$ 中存在 m 个不同的自同构 $\tau_1, \cdots, \tau_m$, 且 $m > n$. 又令 $\{v_1, \cdots, v_n\}$ 为 E 在 F 上的一组基. 由于 $m > n$, 故线性方程组

$$\begin{pmatrix} \tau_1(v_1) & \tau_2(v_1) & \cdots & \tau_m(v_1) \\ \vdots & \vdots & & \vdots \\ \tau_1(v_n) & \tau_2(v_n) & \cdots & \tau_m(v_n) \end{pmatrix} \begin{pmatrix} x_1 \\ \vdots \\ x_m \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$$

在 E 中有非平凡解. 设 $(a_1, a_2, \cdots, a_m)$ 为它的一组非平凡解, 于是对任意的 $j = 1, 2, \cdots, n$, 有

$$\sum_{i=1}^{m} a_i \tau_i(v_j) = 0.$$

因此, 对所有的 $x \in E$, 均有

$$\sum_{i=1}^{m} a_i \tau_i(x) = 0.$$

从而

$$\sum_{i=1}^{m} a_i \tau_i = 0$$

换句话说, $\tau_1, \tau_2, \cdots, \tau_m$ 在 E 上线性相关, 这与引理 3 矛盾.

下面我们回到有限域 k 和 k_n 上来. 考虑 k_n 上将 x 映为 x^q 的映射 σ. 注意到, 对任意的 $x, y \in k_n$, 有

$$\sigma(x + y) = (x + y)^q = x^q + y^q = \sigma(x) + \sigma(y),$$
$$\sigma(xy) = (xy)^q = x^q y^q = \sigma(x)\sigma(y).$$

故 σ 为 k_n 的自同态. 进一步, 对 k_n 中元 x, 若满足 $\sigma(x) = x^q = 1$, 则 $x \neq 0$. 再结合 $x^{q^n - 1} = 1$ 就导出 $x = 1$. 于是 σ 是单射. 又由于 k_n 是有限域, 我们就证明了 σ 为 k_n 上的自同构. 注意到, 对 k 中任意元 x,

$$\sigma(x) = x^q = x,$$

这表明 $\sigma \in \mathrm{Gal}(k_n/k)$. 我们称 σ 为 **Frobenius 自同构**. 设 r 为 σ 的阶，则

$$x = \sigma^r(x) = x^{q^r}, \qquad x \in k_n.$$

又因 $k_n^\times$ 是 $q^n - 1$ 阶循环群，故 $r = n$. 因此 $\mathrm{Gal}(k_n/k)$ 包含了 n 阶循环群 $\langle\sigma\rangle$. 再结合引理 4 即知， $\mathrm{Gal}(k_n/k) = \langle\sigma\rangle$. 此时

$$|\mathrm{Gal}(k_n/k)| = |\langle \sigma \rangle| = n = [k_n : k].$$

即 $\mathrm{Gal}(k_n/k)$ 的阶已达到极大. 在此情况下，称 k_n 为 k 上的 **Galois 扩张**.

总结上面的讨论我们得:

定理 2 域 k_n 是 k 上的 Galois 扩张，其 Galois 群 $\mathrm{Gal}(k_n/k)$ 是由 Frobenius 自同构 σ 生成的 n 阶循环群.

我们注意到： k_n 中的元素 x 位于 k 中的充要条件是它满足 $x^q = x$. 换句话说，它在 Frobenius 自同构作用下不变，亦即它在 Galois 群 $\mathrm{Gal}(k_n/k)$ 作用下不变. 利用 Galois 群 $\mathrm{Gal}(k_n/k)$, 我们可定义两个重要的映射，分别称为关于扩张 k_n/k 的**迹**和**范**, 记作 $\mathrm{Tr}_{k_n/k}$ 和 $\mathrm{N}_{k_n/k}$. 其定义如下:

$$\begin{aligned} \mathrm{Tr}_{k_n/k} : k_n &\longrightarrow k, \\ x &\longmapsto \sum_{\tau \in \mathrm{Gal}(k_n/k)} \tau(x) = \sum_{i=1}^{n} \sigma^i(x) \end{aligned}$$

和

$$\begin{aligned} \mathrm{N}_{k_n/k} : k_n &\longrightarrow k, \\ x &\longmapsto \prod_{\tau \in \mathrm{Gal}(k_n/k)} \tau(x) = \prod_{i=1}^{n} \sigma^i(x). \end{aligned}$$

容易验证，迹和范映射的像均在 k 中，而且可以很明显地看出，$\mathrm{Tr}_{k_n/k}$ 是加法群 k_n 到加法群 k 的同态， $\mathrm{N}_{k_n/k}$ 是乘法群 $k_n^\times$ 到乘法群 $k^\times$ 的同态. 下面我们来研究它们的像.

定理 3 (**Hilbert 定理 90**)　*由乘法群 $k_n^\times$ 到乘法群 $k^\times$ 的范映射 $\mathrm{N}_{k_n/k}$ 是一个满射，且它的核是 $\{x/\sigma(x) : x \in k_n^\times\}$.*

证　由于对任意的 $x \in k_n$,

$$\mathrm{N}_{k_n/k}(\sigma(x)) = \sum_{i=1}^{n} \sigma^{i+1}(x) = \sum_{i=1}^{n} \sigma^{i}(x) = \mathrm{N}_{k_n/k}(x).$$

于是对所有的 $x \in k_n^\times$, $\dfrac{x}{\sigma(x)}$ 位于范映射 $\mathrm{N}_{k_n/k}$ 的核中. 进一步，等式

$$\frac{x}{\sigma(x)} = \frac{y}{\sigma(y)}$$

当且仅当 $xy^{-1} \in k^\times$ 时成立，因此 $\{x/\sigma(x) : x \in k_n^\times\}$ 构成了 $k_n^\times$ 的一个 $\dfrac{q^n-1}{q-1}$ 阶子群，故它等于整个范映射的核的充要条件是，范映射 $\mathrm{N}_{k_n/k}$ 是满射. 为证明这一点，注意到对任意的 $x \in k_n^\times$,

$$\begin{aligned}\mathrm{N}_{k_n/k}(x) &= \prod_{i=1}^{n} \sigma^{i}(x) = x \cdot x^{q} \cdot \cdots \cdot x^{q^{n-1}} \\ &= x^{1+q+\cdots+q^{n-1}} = x^{(q^n-1)/(q-1)}.\end{aligned}$$

于是 $k_n^\times$ 的任意生成元 x 的范 $\mathrm{N}_{k_n/k}(x)$ 的阶是 $q-1$, 即为 $k^\times$ 的生成元，从而范映射 $\mathrm{N}_{k_n/k}$ 是满射.

定理 4(**Hilbert 定理 90**)　*由加法群 k_n 到加法群 k 的迹映射 $\mathrm{Tr}_{k_n/k}$ 是一个满射，且其核为 $\{x-\sigma(x) : x \in k\}$.*

证　由于 $\mathrm{Gal}(k_n/k)$ 中元素是 k 线性映射，故迹映射 $\mathrm{Tr}_{k_n/k}$ 的像 $\mathrm{Tr}_{k_n/k}(k_n)$ 是 k 上的向量空间，因此 $\mathrm{Tr}_{k_n/k}(k_n)$ 或者为 k 或者为 0. 若 $\mathrm{Tr}_{k_n/k}(k_n) = 0$, 则 $\sum\limits_{i=1}^{n} \sigma^{i} = 0$, 这是 $\mathrm{Gal}(k_n/k)$ 中元素的一个非平凡线性关系，由引理 3 知这是不可能的. 于是 $\mathrm{Tr}_{k_n/k}$ 是满射，故其核的势为 q^{n-1}. 明显地

$$\mathrm{Tr}_{k_n/k}(\sigma(x)) = \mathrm{Tr}_{k_n/k}(x),$$

因而核包含有 $\{x-\sigma(x) : x \in k_n\}$. 此外，$y-\sigma(y) = x-\sigma(x)$ 成

立的充要条件为 $x-y\in k$, 于是集合 $\{x-\sigma(x):x\in k_n\}$ 的势是 $q^n/q=q^{n-1}$, 故它等于核.

注 关于范和迹映射的 Hilbert 定理 90 通常是用 Galois 群的一阶上同调来证明的 (参见参考文献 [11]). 在基域有限时, 我们可采用上述方法直接算出.

习题 3 设 k 是一个有限域, k_{mn} 和 k_n 分别为 k 的 mn 次和 m 次有限扩张, 证明

$$\mathrm{Tr}_{k_{mn}/k}=\mathrm{Tr}_{k_m/k}\circ\mathrm{Tr}_{k_{mn}/k_m},$$

$$\mathrm{N}_{k_{mn}/k}=\mathrm{N}_{k_m/k}\circ\mathrm{N}_{k_{mn}/k_m}.$$

给定 k_n 中一元素 z, 它定义了 k_n 上的一个 k 线性变换

$$L_z:x\longmapsto zx,$$

则 L_z 的迹 $\mathrm{Tr}\,L_z$ 和行列式 $\det L_z$ 分别定义为表示线性变换 L_z 的 $n\times n$ 矩阵的迹和行列式. 事实上, 它们由 z 的迹 $\mathrm{Tr}_{k_n/k}(z)$ 和范 $\mathrm{N}_{k_n/k}(z)$ 给出. 精确地讲, 我们有

定理 5 设 $z\in k_n$, 则

(1) $\mathrm{Tr}\,L_z=\mathrm{Tr}_{k_n/k}(z)$, $\det L_z=\mathrm{N}_{k_n/k}(z)$.

(2) 假设 $k(z)=k_n$, 又设 $f(x)=x^n+a_1x^{n-1}+\cdots+a_n$ 为 z 在 k 上的不可约多项式, 那么

$$a_1=-\mathrm{Tr}_{k_n/k}(z)\quad 和\quad a_n=(-1)^n\mathrm{N}_{k_n/k}(z).$$

证 我们将在 $k(z)=k_n$ 的假设下来证定理, 而对 $k(z)$ 为 k_n 的一个真子域时, (1) 的证明留给读者作为练习.

任给 $\tau\in\mathrm{Gal}(k_n/k)$, 由 $0=\tau(f(z))=f(\tau(z))$ 知 $\tau(z)$ 亦为 $f(x)$ 的根. 此外, 若 τ 和 τ' 是 $\mathrm{Gal}(k_n/k)$ 中不同的元素, 则 $\tau(z)$ 与 $\tau'(z)$ 不同 (否则 $k_n=k(z)$ 就不成立了), 这表明 z 在 Galois 群 $\mathrm{Gal}(k_n/k)$ 下有 n 个不同的像, 且均为 $f(x)$ 的根, 从而

$$-a_1=f(x)\ 的根之和=\mathrm{Tr}_{k_n/k}(z),$$

$$(-1)^n a_n = f(x) \text{ 的根之积} = \mathrm{N}_{k_n/k}(z).$$

这就证明了 (2). 对于 (1), 我们已知, L_z 满足 $f(x)=0$, 即 $f(L_z)$ 映 k_n 中的所有元素为 0. 由于 $f(x)$ 在 k 上不可约, 且 $[k_n:k]=n$, 所以 $f(x)$ 为 L_z 的特征多项式. 对应 L_z 的一个表示矩阵可以取作

$$\begin{pmatrix} 0 & 0 & 0 & \cdots & 0 & -a_n \\ 1 & 0 & 0 & \cdots & 0 & -a_{n-1} \\ 0 & 1 & 0 & \cdots & 0 & -a_{n-2} \\ \vdots & \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & -a_2 \\ 0 & 0 & 0 & \cdots & 1 & -a_1 \end{pmatrix}.$$

于是迹为 $-a_1$, 行列式为 $(-1)^n a_n$. 这就证明了 (1).

习题 4 设 $z \in k_n$, 假设 $k(z)=k_m$ 为 k_n 的一个真子域, 证明

$$\mathrm{Tr}\, L_z = \mathrm{Tr}_{k_n/k}(z) = \frac{n}{m}\mathrm{Tr}_{k_m/k}(z),$$

$$\det L_z = \mathrm{N}_{k_n/k}(z) = (\mathrm{N}_{k_m/k}(z))^{n/m}.$$

习题 5 (1) (**正规基定理**) 证明 k_n 中存在一元素 z, 使得

$$\{\tau(z) : \tau \in \mathrm{Gal}(k_n/k)\}$$

是 k_n 在 k 上的一组基.

提示: 考虑 Frobenius 自同构 σ 的最小多项式.

(2) 对 (1) 中的 z, 有 $\mathrm{Tr}_{k_n/k}(z) \neq 0$.

提示: 证明 $\mathrm{Tr}_{k_n/k}(k_n) = k\mathrm{Tr}_{k_n/k}(z)$.

§3 特 征 标

集合 G 称为是 **拓扑群**, 如果 G 既是一个群 (群运算记作乘法), 也是一个拓扑空间, 并且 "映射 $(a,b) \longmapsto ab^{-1}$ 是由 $G \times G$ 至 G 的一个连续映射". 读者可验证这个条件与条件 " G 中乘法运算 $(a,b) \longmapsto ab$ 及求逆运算 $a \longmapsto a^{-1}$ 都是连续的" 是等价的.

我们通常见到的实数域 $\mathbf{R}$ 和复数域 $\mathbf{C}$ 相对于加法和通常的距离拓扑都是拓扑群. 复平面上单位圆 $S^1 = \{z \in \mathbf{C} : |z| = 1\}$ 相对于乘法和 $\mathbf{C}^\times$ 的子空间拓扑也是拓扑群, 并且它是一个紧交换群.

在赋以离散拓扑后, 任意抽象群都是一个拓扑群.

设 G 和 H 都是拓扑群, 若映射 $\phi : G \longrightarrow H$ 既是群同态, 又是连续映射, 则称 ϕ 为连续同态.

拓扑群的概念是将群概念和拓扑空间的概念放在一起而自然产生的, 于是很多群和拓扑空间上的概念与基本关系都可转移到拓扑群上来讨论. 这方面完整的论述可参见经典著作 [7].

在这一节中, 我们着重对拓扑群的特征标进行讨论.

拓扑群 G 的 **特征标** 是由 G 到复平面上单位圆 S^1 的连续同态. 如果 G 是一个有限群, 则它被赋以离散拓扑, 这使得它的特征标简化为由 G 到 S^1 的同态. 由于 S^1 是交换的, 所以群 G 的任意一个特征标在 G 的换位子群 $[G,G]$ 上取值为 1, 因此, 它可看成是商群 $G/[G,G] = G^{ab}$ 的一个特征标. 将群 G 映为 1 的特征标称为 G 的 **平凡特征标**.

例 1 将整数环 $\mathbf{Z}$ 视为一个加法群. S^1 上的任意元素 ξ 定义出 $\mathbf{Z}$ 上的一个特征标 ψ_ξ, 它将整数 n 映至 ξ^n.

例 2 设 N 是一个正整数, 环 $\mathbf{Z}/N\mathbf{Z}$ 中与 N 互素的元素, 也称为环 $\mathbf{Z}/N\mathbf{Z}$ 的单位, 构成一个有限乘法群 $(\mathbf{Z}/N\mathbf{Z})^\times$. 设函数 $\chi : \mathbf{Z} \longrightarrow \mathbf{C}$ 满足

(1) $\chi(n+N) = \chi(n), \quad n \in \mathbf{Z}$;

(2) $\chi(nk) = \chi(n)\chi(k), \quad n, k \in \mathbf{Z}$;

(3) $\chi(n) \neq 0$ 的充要条件是 $\gcd(n, N) = 1$.

则 χ 诱导出环 $\mathbf{Z}/N\mathbf{Z}$ 的单位群 $(\mathbf{Z}/N\mathbf{Z})^\times$ 的一个特征标 (也称为 **$\mathbf{Z}$ 的模 N 的特征标**), 这个函数我们称做 **模 N 的 Dirichlet 特征标**. 反过来, 任何一个群 $(\mathbf{Z}/N\mathbf{Z})^\times$ 的特征标均可扩张为 $\mathbf{Z}$ 上的函数, 使之成为一个模 N 的 Dirichlet 特征标. 今后我们将混用这两个概念.

设 χ_1, χ_2 是拓扑群 G 的两个特征标，定义其积 $\chi_1\chi_2$ 为：

$$\chi_1\chi_2(a) = \chi_1(a)\chi_2(a), \quad a \in G.$$

易证 $\chi_1\chi_2$ 也是 G 的一个特征标. 并且在此运算下，G 上特征标全体构成了一个交换群 $\widehat{G}$, 称之为 G 的**对偶群**. 其中单位圆是平凡特征标，特征标 χ 的逆元是共轭特征标 $\overline{\chi} : a \longmapsto \overline{\chi(a)}$.

例 3 求有限循环群 G 的对偶群 $\widehat{G}$.

设 G 是一个 n 阶循环群，g 是它的生成元. 取 ζ 为一个 n 次本原单位根 (例如可取 $\zeta = \mathrm{e}^{2\pi \mathrm{i}/n}$), 则映 g^j 为 ζ^j 的从 G 到 S^1 的同态 η 是 G 的一个 n 阶特征标. 于是 $\widehat{G}$ 包含了一个 n 阶循环群 $\langle\eta\rangle$. 另一方面，G 的特征标 χ 由它在 g 处的值 $\chi(g)$ 唯一确定. 注意到 $\chi(g)$ 是 n 次单位根，故存在整数 k, 使得 $\chi(g) = \zeta^k$. 由此可推出，$\chi = \eta^k$. 于是 $\widehat{G} = \langle\eta\rangle$ 也是一个 n 阶循环群. 我们看到 $\widehat{G}$ 与 G 同构.

习题 6 求证：$\widehat{\mathbf{Z}} \cong S^1$, $\widehat{\mathbf{R}} \cong \mathbf{R}$.

命题 1 *设 G 是一个有限交换群，则 G 同构于对偶群 $\widehat{G}$.*

证 由有限交换群的基本定理，我们可分解 G 为循环群的乘积 $G = G_1 \times \cdots \times G_r$. 对每个 G 的特征标 χ, 设 χ_i 为它在 G_i 上的限制，则 χ 是 $\chi_1, \cdots, \chi_r$ 的积 $(\chi_1, \cdots, \chi_r)$. 进而可证

$$\widehat{G} = \widehat{G_1} \times \cdots \times \widehat{G_r}$$

由上面例子知道，$\widehat{G}_i$ 与 G_i 同构，故 $\widehat{G}$ 与 G 同构.

注 上述同构 $G \cong \widehat{G}$ 不是典范的 (canonical), 因为它依赖于群分解；而对每个循环群，同构依赖于生成元的选择. 然而 $\widehat{G}$ 的对偶群，记作 $\widehat{\widehat{G}}$, 则自然同构于 G, 这可由

$$\begin{aligned} \xi : G \times \widehat{G} &\longrightarrow S^1, \\ (g, \chi) &\longmapsto \chi(g) \end{aligned}$$

的非退化性得出. 此处应注意到，当固定一个变量时，ξ 关于另一个变量是同态.

习题 7 (1) 证明上述 ξ 是非退化的，即

(a) 若 g 不是 G 中单位元，则存在 G 的特征标 χ, 使得 $\chi(g) \neq 1$.

(b) 若 χ 为 G 的非平凡特征标，则存在 G 中元 g, 使得 $\chi(g) \neq 1$(此为非平凡特征标之定义).

(2) 由 ξ 的非退化性，证明 G 与 $\widehat{\widehat{G}}$ 是自然同构的.

习题 8 对拓扑群 G 的一个闭子群 H, 我们定义 H 的零化子 $H^{\perp}$ 为

$$H^{\perp} = \{\chi \in \widehat{G} : \chi(H) = 1\}.$$

证明当 G 是交换群时，$H^{\perp}$ 典范同构于 $\widehat{G/H}$.

习题 9 设 H 为有限交换群 G 的一个子群，ψ 为 H 的特征标. 证明 ψ 可扩张成为群 G 的一个特征标.

定理 6(Pontrijagin 对偶) 设 G 是一个交换拓扑群，映射 $H \longrightarrow H^{\perp}$ 建立了一个从 G 的闭子群集到 $\widehat{G}$ 的闭子群集间的双射. 进一步，$H^{\perp\perp}$ 同构于 H.

我们仅在 G 为有限交换群时验证此定理，此时拓扑将不起作用. 由有限交换群的基本定理，我们只需就 G 是循环群的情况加以验证，此时 G 的子群集与 G 的阶 $|G|$ 的因子集之间有一个一一对应：$H \longrightarrow |H|$. 注意到 $\widehat{G}$ 亦为 $|G|$ 阶循环群，而 $H^{\perp}$ 的阶是 $|G|/|H|$, 于是映射 $H \longrightarrow H^{\perp}$ 显然为一双射. 在典范同构 $\widehat{\widehat{G}} \longrightarrow G$ 下，我们可将 $H^{\perp\perp}$ 等同于群 G 的子群

$$\widetilde{H} = \{g \in G : \text{对每一个 } \chi \in H^{\perp}, \text{均有 } \chi(g) = 1\}.$$

由于所有的 $\chi \in H^{\perp}$ 在 H 上平凡，故 $\widetilde{H}$ 包含 H. 另一方面，由 $|\widetilde{H}| = |G|/|H^{\perp}|$ 及 $|H^{\perp}| = |G|/|H|$ 导出 $|\widetilde{H}| = |H|$. 于是 $\widetilde{H} = H$, 即 $H^{\perp\perp} \cong H$ 为自然同构.

Pontrijagin 对偶定理的完整论述可见其著作 [7].

在有限群 G 上的复值函数集 $\mathbf{C[G]}$ 上定义内积 $\langle , \rangle$ 如下：

$$\langle f, g \rangle = \frac{1}{|G|} \sum_{x \in G} f(x)\overline{g(x)}.$$

习题 10 证明 $\mathbf{C}[G]$ 关于此内积构成一 Hilbert 空间.

命题 2 设 G 是一有限交换群，则 G 的特征标构成空间 $\mathbf{C}[G]$ 的一组标准正交基.

为此我们先证明关于特征标的两个等式.

引理 5　设 G 是有限交换群, $g \in G$, $\chi \in \widehat{G}$. 则

(1) $$\sum_{x \in G} \chi(x) = \begin{cases} 0, & \text{若 } \chi \text{ 为非平凡特征标}, \\ |G|, & \text{若 } \chi \text{ 为平凡特征标}. \end{cases}$$

(2) $$\sum_{\eta \in \widehat{G}} \eta(g) = \begin{cases} 0, & \text{若 } g \text{ 不是 } G \text{ 的单位元}, \\ |G|, & \text{若 } g \text{ 是 } G \text{ 的单位元}. \end{cases}$$

证　(1) 若 χ 为平凡的, 则结论显然. 现设 χ 为非平凡特征标. 则存在 $y \in G$, 使得 $\chi(y) \neq 1$. 再由

$$\sum_{x \in G} \chi(x) = \sum_{x \in G} \chi(xy) = \chi(y) \sum_{x \in G} \chi(x),$$

即得

$$\sum_{x \in G} \chi(x) = 0.$$

(2) 可由同构 $G \cong \widehat{\widehat{G}}$ 及 (1) 导出.

现在来证命题 2. 设 $\chi_1, \chi_2 \in \widehat{G}$, 由引理 5 知

$$\langle \chi_1, \chi_2 \rangle = \frac{1}{|G|} \sum_{x \in G} \chi_1(x)\overline{\chi_2(x)} = \frac{1}{|G|} \sum_{x \in G} (\chi_1\chi_2^{-1})(x)$$
$$= \begin{cases} 0, & \text{若 } \chi_1 \neq \chi_2, \\ 1, & \text{若 } \chi_1 = \chi_2. \end{cases}$$

这表明 G 的特征标构成一标准正交集, 因而是线性独立的. 另一方面, $|\widehat{G}| = |G| = \dim_{\mathbf{C}} \mathbf{C}[G]$, 于是这些特征标构成了一组标准正交基.

§4　有限域上的特征标及 Gauss 和

在本节中, 设 k 是一个有 $q = p^d$ 个元素的有限域, 其中 p 为素数. 由 §1 中讨论可以看出, 加法群 k 是 d 个 p 阶循环群的直和, 因此 k 的加法特征标群 $\widehat{k}$ 有同样结构.

例 4 对于素域 $F_p = \mathbf{Z}/p\mathbf{Z}$, 映 x 为 $\psi(x) = \mathrm{e}^{2\pi \mathrm{i}x/p}$ 的映射 $\psi : F_p \longrightarrow S^1$ 是它的一个加法特征标, 且 $\widehat{F_p} = \langle \psi \rangle$.

我们已知迹映射 $\mathrm{Tr}_{k/F_p} : k \longrightarrow F_p = \mathbf{Z}/p\mathbf{Z}$ 是加法群同态, 于是对每个 $\phi \in \widehat{F_p}$, 有 $\phi \circ \mathrm{Tr}_{k/F_p} \in \widehat{k}$. 又由于迹映射是满射, 于是每个 F_p 的非平凡特征标通过结合迹映射而成为 k 的一个非平凡加法特征标.

命题 3 设 ψ 是有限域 k 的一个非平凡加法特征标. 对 $a \in k$, 定义 $\psi^a : k \longrightarrow S^1$ 为 $\psi^a(x) = \psi(ax)$. 则 ψ^a 是 k 的一个加法特征标, 并且 $a \longmapsto \psi^a$ 给出一个从 k 到 $\widehat{k}$ 的同构. 特别地, $\widehat{k} = \{\psi^a : a \in k\}$.

证 以 L_a 表示 k 上乘 a 的线性变换

$$x \longmapsto L_a(x) = ax,$$

则 $\psi^a = \psi \circ L_a$. 若 $a = 0$, 则 $L_a = 0$, 故 ψ^a 为 k 上平凡特征标; 若 $a \neq 0$, 则 L_a 是加法群 k 的一个自同构, 于是 ψ^a 为一个非平凡加法特征标. 对 $a, b \in k$, 有 $\psi^{a+b} = \psi^a \psi^b$, 因此 $a \longmapsto \psi^a$ 是由 k 到 $\widehat{k}$ 的单同态, 又因 $|\widehat{k}| = |k|$, 故这个同态也是满的.

例 5 以 Ψ 表示特征标 $\psi \circ \mathrm{Tr}_{k/F_p}$. 则由命题 3 知

$$\widehat{k} = \{\Psi^a : a \in k\}.$$

习题 11 令 V 是域 k 上的有限维向量空间, $v_1, \cdots, v_n$ 为它的一组基. 定义由 $V \times V$ 至 k 的双线性形式 $\langle\ ,\ \rangle$ 为

$$\langle x, y \rangle = \sum_{i=1}^{n} x_i y_i,$$

此处 $x = x_1 v_1 + \cdots + x_n v_n$, $y = y_1 v_1 + \cdots + y_n v_n$, $x_i, y_i \in k$. 令 ψ 为 k 的一个非平凡加法特征标. 对每个 $v \in V$, 定义 V 上之特征标 ψ^v 为 $\psi^v(x) = \psi(\langle v, x \rangle)$. 证明: $\widehat{V} = \{\psi^v : v \in V\}$.

乘法群 $k^\times$ 的乘法特征标群 $\widehat{k^\times}$ 是一个 $q-1$ 阶循环群, 群 $k^\times$ 的任意特征标 χ 可如下扩充为空间 $\mathbf{C}[k]$ 中的元:

$$\chi(0)=\begin{cases}0, & 若\ \chi\ 是非平凡的,\\ 1, & 若\ \chi\ 是平凡的.\end{cases}$$

由命题 2 知，它可写成 k 上加法特征标的线性组合，其系数称为**正规化 Gauss 和**. 精确地说，对非平凡乘法特征标 χ，我们有

$$\chi=\sum_{\psi\in\widehat{k}}\langle\chi,\overline{\psi}\rangle\overline{\psi}=\sum_{\psi\in\widehat{k}}{}'\langle\chi,\overline{\psi}\rangle\overline{\psi}=\frac{1}{|k|}\sum_{\psi\in\widehat{k}}{}'g(\chi,\psi)\overline{\psi}. \tag{4.1}$$

其中 $\sum'$ 表示除去平凡元，$g(\chi,\psi)$ 称为 **χ 关于 ψ 的 Gauss 和**，其定义为

$$g(\chi,\psi)=|k|\langle\chi,\overline{\psi}\rangle=\sum_{x\in k^\times}\chi(x)\psi(x). \tag{4.2}$$

(4.1) 式可视为乘法特征标 χ 关于加法特征标的 Fourier 展开，而 (4.2) 式中的 Gauss 和则为该 Fourier 展开的 Fourier 系数.

(4.2) 式所定义的 Gauss 和可一般化为对 χ 与 ψ 不加限制. 容易看出，此时有

$$g(\chi,\psi)=\begin{cases}q-1, & 若\ \chi\ 和\ \psi\ 均为平凡特征标;\\ -1, & 若\ \chi\ 为而\ \psi\ 不为平凡特征标;\\ 0, & 若\ \psi\ 为而\ \chi\ 不为平凡特征标.\end{cases}$$

命题 4　设 $\chi\in\widehat{k^\times}, \psi\in\widehat{k}$ 均为非平凡特征标，则

(1) $g(\chi,\psi)g(\overline{\chi},\psi)=|k|\chi(-1)=q\chi(-1)$,

(2) $\overline{g(\chi,\psi)}=\chi(-1)g(\overline{\chi},\psi)$.

于是 Gauss 和 $g(\chi,\psi)$ 的绝对值为 $\sqrt{q}$.

证　(1) 由定义

$$\begin{aligned}g(\chi,\psi)g(\overline{\chi},\psi)&=\sum_{x\in k^\times}\chi(x)\psi(x)\sum_{y\in k^\times}\overline{\chi}(y)\psi(y)\\&=\sum_{x\in k^\times}\chi(x)\psi(x)\sum_{z\in k^\times}\overline{\chi}(xz)\psi(xz)\qquad(令\ y=xz)\end{aligned}$$

$$= \sum_{x\in k^\times} \overline{\chi}(z)\left(\sum_{x\in k}\psi((1+z)x)-\psi(0)\right)$$

$$= \sum_{z\in k^\times} \overline{\chi}(z)\left(\sum_{x\in k}\psi^{1+z}(x)-1\right)$$

$$= \sum_{z\in k^\times} \overline{\chi}(z)\sum_{x\in k}\psi^{1+z}(x).$$

最后一步用到对非平凡特征标 χ, $\sum\limits_{z\in k^\times}\chi(z)=0$ (引理 5). 再次运用引理 5 于加法群 k 可得

$$\sum_{x\in k}\psi^{1+z}(x)=\begin{cases}0, & 若1+z\neq 0,\\ q, & 若1+z=0.\end{cases}$$

于是 $g(\chi,\psi)g(\overline{\chi},\psi)=q\chi(-1)$, 如命题所述.

(2) 由定义, 直接计算, 有

$$\overline{g(\chi,\psi)}=\sum_{x\in k^\times}\overline{\chi(x)\psi(x)}=\sum_{x\in k^\times}\overline{\chi}(x)\psi(-x)$$
$$=\chi(-1)\sum_{x\in k^\times}\overline{\chi}(x)\psi(x)$$
$$=\chi(-1)g(\overline{\chi},\psi).$$

一般情况下, 计算 $g(\chi,\psi)/\sqrt{q}$ 是一件很困难的工作.

习题 12 设 N 是一个正整数, m 为 N 的一个正因子, χ 是 $\mathbf{Z}$ 的模 N 的特征标. 证明下面条件彼此等价:

(1) 存在 $\mathbf{Z}$ 的模 m 的特征标 χ', 使得对任意与 N 互素的整数 a 有 $\chi(a)=\chi'(a)$;

(2) 当 $\gcd(a,N)=1$ 且 $a\equiv 1 \pmod m$ 时, 有 $\chi(a)=1$.

(3) 当 $\gcd(a,N)=\gcd(a',N)=1$ 且 $a\equiv a' \pmod m$ 时, 有 $\chi(a)=\chi(a')$.

若不存在 N 的任意真因子 m 使得习题 12 中的条件成立, 则我们称特征标 χ 是**模 N 的本原特征标**, N 称为 χ 的**前导子**.

习题 13 设 N 的是一个大于 1 的正整数, $\psi_N(x)=e^{2\pi ix/N}$ 为加法群 $\mathbf{Z}/N\mathbf{Z}$ 上的加法特征标.

(1) 设 χ 是 $\mathbf{Z}$ 的模 N 的本原特征标, 证明 Gauss 和

$$g(\chi,\psi_N)=\sum_{x(\bmod N)}\chi(x)\psi_N(x)$$

的绝对值是 $\sqrt{N}$.

(2) 设 χ_1, χ_2 分别为 $\mathbf{Z}$ 的模 N_1, N_2 的本原特征标, 证明唯一存在前导子为 N 的特征标 χ, 使得

(a) $N|N_1N_2$;

(b) $\chi(a)=\chi_1(a)\chi_2(a)$, 对所有的 $a\in\mathbf{Z}$, 且 $\gcd(a,N_1N_2)=1$.

通常将 χ 记作 $\chi_1\chi_2$, 称为 χ_1 和 χ_2 的积.

(3) 条件同 (2), 并且 N_1, N_2 互素. 证明 $\chi_1\chi_2$ 的前导子为 N_1N_2, 它在 $(\mathbf{Z}/N_i\mathbf{Z})^\times$ 上的限制是 $\chi_i(i=1,2)$. 此外, 试找出 Gauss 和 $g(\chi_1\chi_2,\psi_{N_1N_2})$ 与 $g(\chi_1,\psi_{N_1})$ 和 $g(\chi_2,\psi_{N_2})$ 之间的关系.

Gauss 和 $g(\chi,\psi)$ 在视为 χ 和 ψ 的函数时, 关于 ψ 的变化是很简单的. 事实上, 固定一个非平凡加法特征标 ψ, 则其他非平凡加法特征标都可写作 $\psi^t(t\in k^\times)$ 的形式, 从而

$$\begin{aligned}g(\chi,\psi^t)&=\sum_{x\in k^\times}\chi(x)\psi^t(x)=\sum_{x\in k^\times}\chi(x)\psi(tx)\\&=\chi(t)^{-1}\sum_{x\in k^\times}\chi(tx)\psi(tx)=\chi(t)^{-1}g(\chi,\psi).\end{aligned}\tag{4.3}$$

于是公式 (4.1) 可化成

$$\chi=\frac{1}{|k|}\sum_{t\in k^\times}g(\chi,\psi^t)\overline{\psi^t}=\frac{1}{|k|}g(\chi,\psi)\sum_{t\in k^\times}\chi(t)^{-1}\overline{\psi^t}.\tag{4.4}$$

Gauss 和 $g(\chi,\psi)$ 作为 χ 的函数, 其变化要复杂得多. 在 χ_1, χ_2 和 $\chi_1\chi_2$ 都是非平凡时,

$$\frac{g(\chi_1,\psi)g(\chi_2,\psi)}{g(\chi_1\chi_2,\psi)}=\sum_{\substack{s,t\in k\\s+t=1}}\chi_1(s)\chi_2(t)=\chi_1\chi_2(-1)\sum_{\substack{s,t\in k\\s+t+1=0}}\chi_1(s)\chi_2(t)$$

(等式的证明是直接的, 留给读者作为练习). 注意等式右边与 ψ 无关, 这也可从等式左边并利用 (4.3) 式得出, 它被称为关于 χ_1 和 χ_2 的 **Jacobi 和**, 记作 $j(\chi_1,\chi_2)$. 更一般地, 设 $\chi_1,\cdots,\chi_r$ 的为 $k^\times$ 的一组非平凡特征标, 关于 $\chi_1,\cdots,\chi_r$ 的 **Jacobi 和** 定义为

$$j(\chi_1,\cdots,\chi_r)=\sum_{\substack{v_1,\cdots,v_r\in k^\times\\ v_1+\cdots+v_r+1=0}}\chi_1(v_1)\cdots\chi_r(v_r).$$

习题 14 设 $\chi_0=(\chi_1\cdots\chi_r)^{-1}$. 证明

$$j(\chi_1,\cdots,\chi_r)=(q-1)^{-1}\sum_{\substack{v_0,\cdots,v_r\in k^\times\\ v_0+\cdots+v_r=0}}\chi_0(v_0)\chi_1(v_1)\cdots\chi_r(v_r).$$

命题 5 设 $\chi_0,\chi_1,\cdots,\chi_r$ 是 $k^\times$ 的非平凡特征标, 使得

$$\chi_0\chi_1\cdots\chi_r=1.$$

则对 k 的任意非平凡加法特征标 ψ, 有

$$j(\chi_1,\cdots,\chi_r)=\frac{1}{q}g(\chi_0,\psi)g(\chi_1,\psi)\cdots g(\chi_r,\psi).$$

特别地, $j(\chi_1,\cdots,\chi_r)$ 的绝对值为 $q^{(r-1)/2}$.

证 对固定的 k 的非平凡加法特征标 ψ, 将 χ_i 按 (4.4) 式那样写成 ψ^t 的线性组合

$$\chi_i=\frac{1}{q}g(\chi_i,\psi)\sum_{t\in k^\times}\overline{\chi_i}(t)\overline{\psi}^{\,t}.$$

将此式代入习题 14 中 $j(\chi_1,\cdots,\chi_r)$ 的表达式得

$$\begin{aligned}&(q-1)j(\chi_1,\cdots,\chi_r)\\ &\quad=q^{-r-1}g(\chi_0,\psi)\cdots g(\chi_r,\psi)\\ &\qquad\times\sum_{\substack{u_i\in k\\ u_0+\cdots+u_r=0}}\sum_{t_i\in k^\times}\overline{\chi_0}(t_0)\cdots\overline{\chi_r}(t_r)\overline{\psi}(t_0u_0+\cdots+t_ru_r).\end{aligned}$$

但对固定的 $t_0,\cdots,t_r$, 由引理 5 知

$$\begin{aligned}
&\sum_{\substack{u_i\in k\\u_0+\cdots+u_r=0}} \overline{\psi}(t_0u_0+\cdots+t_ru_r)\\
&\quad=\sum_{u_i}\overline{\psi}(t_0(u_0+\cdots+u_r)+(t_1-t_0)u_1+\cdots+(t_r-t_0)u_r)\\
&\quad=\sum_{u_1,\cdots,u_r\in k}\overline{\psi}((t_1-t_0)u_1)\cdots\overline{\psi}((t_r-t_0)u_r)\\
&\quad=\begin{cases} q^r, & \text{若 } t_0=t_1=\cdots=t_r,\\ 0, & \text{其他}.\end{cases}
\end{aligned}$$

于是

$$\begin{aligned}
&(q-1)j(\chi_1,\cdots,\chi_r)\\
&\quad=q^{-1}g(\chi_0,\psi)\cdots g(\chi_r,\psi)\sum_{t_0\in k^\times}(\overline{\chi_0}\cdots\overline{\chi_r})(t_0)\\
&\quad=\frac{q-1}{q}g(\chi_0,\psi)\cdots g(\chi_r,\psi).
\end{aligned}$$

这里用到 $\chi_0\chi_1\cdots\chi_r=1$. 由此命题得证.

习题 15 当 $\chi_1\cdots\chi_r=1$ 时, 证明

$$j(\chi_1,\cdots,\chi_r)=-q^{-1}g(\chi_1,\psi)\cdots g(\chi_r,\psi).$$

特别地, $|j(\chi_1,\cdots,\chi_r)|=q^{\frac{r}{2}-1}$.

§5　Davenport-Hasse 等式

在本节中, k 是一个有限域, χ 为 $k^\times$ 的一个非平凡乘法特征标, ψ 是 k 的非平凡加法特征标. 对一个正整数 ν, 我们以 k_ν 表示 k 的 ν 次域扩张. 回忆一下在 §2 中讨论过的迹映射 $\mathrm{Tr}_{k_\nu/k}$ 和范映射 $\mathrm{N}_{k_\nu/k}$, 它们分别是域 k_ν 与 k 的加法群和乘法群之间的满同态. 因此 $\chi=\chi\circ\mathrm{N}_{k_\nu/k}$ 是 $k_\nu^\times$ 的一个非平凡乘法特征标,

$\Psi=\psi\circ\mathrm{Tr}_{k_\nu/k}$ 是 k_ν 的非平凡加法特征标. 从而我们有两个 Gauss 和

$$g(\chi,\psi)=\sum_{y\in k^\times}\chi(y)\psi(y)$$

与

$$g(\chi,\Psi)=\sum_{y\in k_\nu^\times}\chi(y)\Psi(y).$$

它们之间满足下面关系:

定理 7(Davenport-Hasse[1]) $-g(\chi,\Psi)=(-g(\chi,\psi))^\nu$.

下面的证明取材于 A. Weil 的文章 [10]. 对 k 上每个有非 0 常数项的首一多项式

$$f(x)=x^n+a_{n-1}x^{n-1}+\cdots+a_0,\qquad a_i\in k,\ a_0\neq 0,$$

定义

$$\lambda(f)=\chi(a_0)\psi(a_{n-1}).$$

容易证明, 若 f_1, f_2 是两个这样的多项式, 则

$$\lambda(f_1f_2)=\lambda(f_1)\lambda(f_2).$$

由于任何这样的多项式都是不可约多项式的积, 于是形式上有下面等式

$$\sum_{\substack{f(x)\in k[x]\\ f\text{首一},\ f(0)\neq 0}}\lambda(f)u^{\deg f}=\prod_{p\in\Xi(k)}\left(1-\lambda(p)u^{\deg p}\right)^{-1},\tag{5.1}$$

其中

$$\Xi(k)=\{p(x)\in k[x]:p\text{ 为首一不可约的, 且 }p(0)\neq 0\}.$$

首先我们计算 (5.1) 式左边的和式. 设 $d\geq 2$, 现研究固定 $a_{d-2},\cdots,a_0\in k, a_0\neq 0$ 之多项式集

$$\begin{aligned}S&=S(a_{d-2},\cdots,a_0)\\&=\{f(x)=x^n+a_{d-1}x^{n-1}+\cdots+a_0:a_{d-1}\in k\}.\end{aligned}$$

容易证明，$\sum_{f \in S} \lambda(f) = 0$, 进而导出 (5.1) 式左边只是一个次数 ≤ 1 的多项式. 另一方面，出现于 (5.1) 式左边的一次多项式的形式为 $x + a$, $a \in k^{\times}$, 所以 u 的系数为

$$\sum_{a \in k^{\times}} \lambda(x + a) = \sum_{a \in k^{\times}} \chi(a)\psi(a) = g(\chi, \psi).$$

此外，注意到 (5.1) 式左边常数项系数为 1, 于是我们就证明了

$$1 + g(\chi, \psi)u = \prod_{p \in \Xi(k)} \left(1 - \lambda(p)u^{\deg p}\right)^{-1}. \tag{5.2}$$

类似地，对 $F(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in k_\nu[x]$ 且 $a_0 \neq 0$, 我们定义

$$\Lambda(F) = \mathcal{X}(a_{n-1})\Psi(a_0).$$

同样地有

$$1 + g(\mathcal{X}, \Psi)U = \prod_{P \in \Xi(k_\nu)} \left(1 - \Lambda(p)U^{\deg P}\right)^{-1}. \tag{5.3}$$

我们来研究 (5.2) 与 (5.3) 式中的无限乘积. 设 $p(x)$ 为 $k[x]$ 中的首一不可约多项式，$P(x)$ 为 $k_\nu[x]$ 中的首一不可约多项式，$P(x)|p(x)$. 则对任意的 $\tau \in \mathrm{Gal}(k_\nu/k)$, $\tau(P(x))$ 可整除 $\tau(p(x)) = p(x)$, 且 $\tau(P(x))$ 亦为 $k_\nu[x]$ 中的首一不可约多项式. 设 $\tau_1(P(x))$, $\cdots$,$\tau_r(P(x))$ 为 $P(x)$ 在 $\mathrm{Gal}(k_\nu/k)$ 作用下不同的像，则它们都是 $k_\nu[x]$ 中 $p(x)$ 的不可约因子，其积 $q(x) = \tau_1(P(x))\cdots\tau_r(P(x))$ 也整除 $p(x)$, 且在 $\mathrm{Gal}(k_\nu/k)$ 作用下不变. 于是 $q(x) \in k[x]$. 又由于 $p(x)$ 不可约，且它们都是首一的，故 $q(x) = p(x)$. 换句话说，

$$p(x) = \tau_1(P(x))\cdots\tau_r(P(x))$$

是 $P(x)$ 在 $\mathrm{Gal}(k_\nu/k)$ 下共轭元的积. 这表明 $k[x]$ 中每一个首一不可约多项式可分解为 $k_\nu[x]$ 中不同的且在 $\mathrm{Gal}(k_\nu/k)$ 下共轭的首一不可约多项式的积；每个 $k_\nu[x]$ 中的首一不可约多项式则可整除唯

一的一个 $k[x]$ 中首一不可约多项式. 于是我们有

$$1+g(\chi,\Psi)U=\prod_{p\in\Xi(k)}\prod_{\substack{P\in\Xi(k_\nu)\\P|p}}\left(1-\Lambda(P)U^{\deg P}\right)^{-1}.$$

下面我们固定 $k[x]$ 中一个 n 次首一不可约多项式 $p(x)$, 且 $p(0)\neq 0$. 设 $P(x)$ 为 $p(x)$ 在 $k_\nu[x]$ 中的一个首一不可约因子. 我们来研究 $\lambda(p)$ 和 $\Lambda(P)$ 之间的关系. 设 $-\xi$ 是 $P(x)$ 在一个 k_ν 的代数闭包 $\overline{k_\nu}$ 中的根. 则 $p(x)$ 为 $-\xi$ 在 k 上的不可约多项式, $P(x)$ 为 $-\xi$ 在 k_ν 上的不可约多项式. 设 $k(\xi)\bigcap k_\nu$ 在 k 上的次数是 d(图 1). 由于在 $\overline{k_\nu}$ 中, 对给定的自然数 d, 仅存在唯一一个 k 上的 d 次域扩张, 因此 $d=\gcd(n,\nu)$(从而 n/d 与 ν/d 互素). 于是

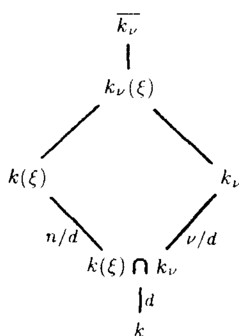


图 1

$$\deg P=[k_\nu(\xi):k_\nu]=[k(\xi):k(\xi)\bigcap k_\nu]=\frac{n}{d},$$

且 $p(x)$ 在 $k_\nu[x]$ 中有 d 个不同的首一不可约因子. 记

$$p(x)=x^n+bx^{n-1}+\cdots+a,$$
$$P(x)=x^{n/d}+Bx^{n/d-1}+\cdots+A.$$

由定理 5 知

$$b=-\mathrm{Tr}_{k(\xi)/k}(-\xi)=\mathrm{Tr}_{k(\xi)/k}(\xi),$$
$$a=(-1)^n\mathrm{N}_{k(\xi)/k}(-\xi)=\mathrm{N}_{k(\xi)/k}(\xi),$$

同理

$$B=\mathrm{Tr}_{k_\nu(\xi)/k_\nu}(\xi),\quad A=\mathrm{N}_{k_\nu(\xi)/k_\nu}(\xi).$$

于是

$$\lambda(p)=\chi(a)\psi(b)=\chi(\mathrm{N}_{k(\xi)/k}(\xi))\psi(\mathrm{Tr}_{k(\xi)/k}(\xi)),$$

$$\begin{aligned}\Lambda(P) &= \mathcal{X}(A)\Psi(B) = \mathcal{X}(\mathrm{N}_{k_\nu(\xi)/k_\nu}(\xi))\Psi(\mathrm{Tr}_{k_\nu(\xi)/k_\nu}(\xi)) \\ &= \chi(\mathrm{N}_{k_\nu(\xi)/k}(\xi))\psi(\mathrm{Tr}_{k_\nu(\xi)/k}(\xi)) \\ &= \chi(\mathrm{N}_{k(\xi)/k}(\xi))^{\nu/d}\psi(\mathrm{Tr}_{k(\xi)/k}(\xi))^{\nu/d} = \lambda(p)^{\nu/d}.\end{aligned}$$

由此

$$\prod_{\substack{P\in\Xi(k_\nu)\\ P|p}} \left(1 - \Lambda(P)U^{\deg P}\right)^{-1} = \left(1 - \lambda(p)^{\nu/d}U^{n/d}\right)^{-d}.$$

将 u^ν 代换 U, 则

$$\begin{aligned}\left(1-\lambda(p)^{\nu/d}U^{n/d}\right)^{-d} &= \left(1 - \lambda(p)^{\nu/d}u^{n\nu/d}\right)^{-d} \\ &= \prod_{i=1}^{\nu/d}\left(1 - \lambda(p)\zeta_{\nu/d}^{i}u^n\right)^{-d} = \prod_{i=1}^{\nu}\left(1 - \lambda(p)(\zeta_\nu^i u)^n\right)^{-1},\end{aligned}$$

其中 ζ_m 表 m 次本原单位根. 于是

$$\begin{aligned}1+g(\mathcal{X},\Psi)u^\nu &= \prod_{p\in\Xi(k)}\prod_{i=1}^{\nu}\left(1 - \lambda(p)(\zeta_\nu^i u)^{\deg p}\right)^{-1} \\ &= \prod_{i=1}^{\nu}(1 + g(\chi,\psi)\zeta_\nu^i u) \qquad (\text{利用 (5.2) 式}) \\ &= 1 - (-g(\chi,\psi))^\nu u^\nu.\end{aligned}$$

由此定理得证.

习题 16 设 $\chi_1,\cdots,\chi_r$ 为 $k^\times$ 的非平凡特征标, $\mathcal{X}_1,\cdots,\mathcal{X}_r$ 为 $\chi_1,\cdots,\chi_r$ 与范映射合成而得到的 $k_\nu^\times$ 上的非平凡特征标. 试找出 Jacobi 和 $j(\chi_1,\cdots,\chi_r)$ 与 Jacobi 和 $j(\mathcal{X}_1,\cdots,\mathcal{X}_r)$ 之间的关系.

参 考 文 献

[1] H. Davenport and H. Hasse, *Die Nullstellen der Kongruenzetafunktionen in gewissen zyklischen Fallen*, J. reine und angew. Math., 172(1935), 151~182.

[2] 冯克勤，《有限域》，湖南科技出版社，长沙，1991.

[3] N. Jacobson, *Basic Algebra* I, Freeman, San Francisco, 1980. (中译本：《基础代数》，一卷，一、二分册，高教出版社，北京，1988.)

[4] 黎景辉、冯绪宁，《拓扑群引论》，科学出版社，北京，1991.

[5] S. Lang, *Algebra*, Addison-Wesley, Reading Mass., 1967.

[6] R. Lidel and H. Niederreiter, *Finite Fields*, Addison-Wesley, Reading Mass., 1983.

[7] Л. С. Понтрягин, Непрерывные Группы, Москва, 1954. (中译本：《连续群》(上、下)，科学出版社，北京，1957.)

[8] J. P. Serre, *A Course in Arithmetic*, GTM 7, Springer-Verlag, New York, 1973. (中译本：《数论教程》，上海科技出版社，上海，1980.)

[9] B. L. van der Warden, *Algebra* (I, II), Springer-Verlag, Berlin, 1955, 1959. (中译本：《代数学》(I, II)，科学出版社，北京，1963, 1976.)

[10] A. Weil, *Numbers of solutions of equations in finite fields*, Bull. Amer. Math. Soc., **55**(1949), 497~508.

[11] D. Winter, *The Structure of Fields*, GTM 16, Springer-Verlag, New York, 1974.

第二章　Weil 猜想

在本章中，如无特殊说明，k 总表示一个有 q 个元素的有限域，$k^\times$ 表示它的所有非零元素组成的乘法群.

§1　有限域上方程的解数

在这一节里，我们将讨论华罗庚-Vandiver[12] 和 Weil[14] 独立做出的关于有限域上多项式方程解数的估计. 这里我们是按 Weil[14] 的思想来进行讨论，因为这将导出著名的 Weil 猜想的表述.

考虑下面类型的方程

$$a_0x_0^{n_0}+a_1x_1^{n_1}+\cdots+a_rx_r^{n_r}=b,$$

其中 $a_i\in k^\times$，$b\in k$，$n_0,n_1,\cdots,n_i$ 为正整数，我们希望能对该方程在 k^{r+1} 中解的个数有个估计.

首先我们研究 $b=0$ 的情况. 给定 $u\in k$，以 $N_i(u)$ 表示方程 $x^{n_i}=u$ 在 k 中解的个数. 显然，$N_i(0)=1$. 又设 d_i 是 n_i 与 $q-1$ 的最大公因子. 由于 $k^\times$ 是一个 $q-1$ 阶循环群，那么当 u 是 $k^\times$ 中某个元的 d_i 次幂时，$N_i(u)=d_i$；否则 $N_i(u)=0$.

以 N 表示方程

$$a_0x_0^{n_0}+a_1x_1^{n_1}+\cdots+a_rx_r^{n_r}=0$$

在 k^{r+1} 中的解数. 则

$$N=\sum_{\substack{u_i\in k\\ \sum a_iu_i=0}}N_0(u_0)N_1(u_1)\cdots N_r(u_r). \tag{1.1}$$

此处我们应注意到满足 $\sum a_iu_i=0$ 的 $r+1$ 元组 $(u_0,u_1,\cdots,u_r)$ 集合构成了 k 上的一个 r 维向量空间.

函数 N_i 可进一步用 $k^\times$ 的特征标来表示. 以 H_i 表示 $k^\times$ 的子群 $(k^\times)^{n_i}=(k^\times)^{d_i}$, 这是一个 $(q-1)/d_i$ 阶循环群. 又由于 $H_i^\perp$ 的阶为 d_i, 且它包含了 $\widehat{k^\times}$ 中所有满足 $\chi^{d_i}=1$ 的特征标 χ, 因此它就等于集合 $\{\chi\in\widehat{k^\times}|\chi^{d_i}=1\}$. 将 $k^\times$ 的特征标 χ 扩张成 k 上的函数 (参阅第一章 §4), 我们定义它在 0 处的值如下:

$$\chi(0)=\begin{cases}0, & \text{若 } \chi \text{ 是非平凡的,}\\ 1, & \text{若 } \chi \text{ 是平凡的.}\end{cases}$$

于是, 对任意的 $u\in k$,

$$\sum_{\chi\in H_i^\perp}\chi(u)=\begin{cases}1, & \text{若 } u=0,\\ d_i=|H_i^\perp|, & \text{若 } u\in H_i,\\ 0, & \text{其他.}\end{cases}$$

这里用到了在第一章讨论过的 $H_i^{\perp\perp}=H_i$ 这一结论. 换句话说, 作为一个 k 上的函数, N_i 可以表示成

$$N_i=\sum_{\chi\in H_i^\perp}\chi=\sum_{\substack{\chi\in\widehat{k^\times}\\ \chi^{d_i}=1}}\chi.$$

将它代入解数 N 的计算式 (1.1) 中, 我们得到下面 N 的表法

$$N=\sum_{\substack{u_i\in k\\ \sum a_iu_i=0}}\ \sum_{\substack{\chi_i\in\widehat{k^\times}\\ \chi_i^{d_i}=1}}\chi_0(u_0)\chi_1(u_1)\cdots\chi_r(u_r).$$

为了得到对 N 的估计, 我们将首先固定 $(\chi_0,\chi_1,\cdots,\chi_r)$, 然后对 u_i 来求和. 若所有的 χ_i 是平凡的, 则对任意的 $u\in k$, 有

$$\chi_i(u)=1.$$

因此, 对使 $\sum a_iu_i=0$ 的 u_i 求和恰是线性方程 $\sum a_iu_i=0$ 的解数, 它等于 q^r. 下面假设存在某一特征标 χ_{i_0} 平凡, 但并非所有的特征标都是平凡的. 注意到 $\chi_{i_0}(u_{i_0})$ 与 u_{i_0} 无关. 于是上面这个关

于 u_i (其中 u_i 满足 $\sum a_i u_i = 0$) 的和式就变为

$$\prod_{\substack{j \neq i_0 \\ 0 \leq j \leq r}} \left(\sum_{u_j \in k} \chi_j(u_j) \right).$$

又由于其中至少有一个非平凡特征标，故此乘积等于 0. 这样我们就得到了

$$
\begin{aligned}
N &= q^r + \sum_{\substack{u_i \in k \\ \sum a_i u_i = 0}} \sum_{\substack{\chi_i \in \widehat{k^\times} \\ \chi_i \neq 1 \\ \chi_i^{d_i} = 1}} \chi_0(u_0)\chi_1(u_1)\cdots\chi_r(u_r) \\
&= q^r + \sum_{\substack{\chi_i \in \widehat{k^\times} \\ \chi_i \neq 1 \\ \chi_i^{d_i} = 1}} \chi_0(a_0)^{-1}\cdots\chi_r(a_r)^{-1} \\
&\quad \times \sum_{\substack{y_i \in k^\times \\ \sum y_i = 0}} \chi_0(y_0)\cdots\chi_r(y_r) \qquad (\text{令 } y_i = a_i u_i) \\
&= q^r + \sum_{\substack{\chi_i \neq 1 \\ \chi_i^{d_i} = 1}} \chi_0(a_0)^{-1}\cdots\chi_r(a_r)^{-1} \\
&\quad \times \sum_{\substack{y_0, v_i \in k^\times \\ 1 + v_1 + \cdots + v_r = 0}} (\chi_0\cdots\chi_r)(y_0)\chi_1(v_1)\cdots\chi_r(v_r) \quad (\text{令 } y_i = y_0 v_i) \\
&= q^r + (q-1) \sum_{\substack{\chi_0\cdots\chi_r = 1 \\ \chi_i \neq 1 \\ \chi_i^{d_i} = 1}} \chi_0(a_0)^{-1}\cdots\chi_r(a_r)^{-1} \\
&\quad \times \sum_{\substack{v_i \in k^\times \\ 1 + v_1 + \cdots + v_r = 0}} \chi_1(v_1)\cdots\chi_r(v_r)
\end{aligned}
$$

$$= q^r + (q-1) \sum_{\substack{\chi_0 \cdots \chi_r = 1 \\ \chi_i \neq 1 \\ \chi_i^{d_i} = 1}} \chi_0(a_0)^{-1} \cdots \chi_r(a_r)^{-1} j(\chi_1, \cdots, \chi_r).$$

这里用到 Jacobi 和 $j(\chi_1, \cdots, \chi_r)$ 的定义与

$$\sum_{y_0 \in k^\times} (\chi_0\chi_1 \cdots \chi_r)(y_0) = \begin{cases} 0, & 若\ \chi_0\chi_1 \cdots \chi_r \neq 1, \\ q-1, & 若\ \chi_0\chi_1 \cdots \chi_r = 1. \end{cases}$$

利用第一章命题 5, 对任意 k 的非平凡加法特征标 ψ, Jacobi 和可表为

$$j(\chi_1, \cdots, \chi_r) = q^{-1} g(\chi_0, \psi) \cdots g(\chi_r, \psi),$$

且其绝对值为 $q^{(r-1)/2}$, 这里 $\chi_0 = (\chi_1 \cdots \chi_r)^{-1}$. 命

$$S(d_0, \cdots, d_r) = \{(\chi_0, \cdots, \chi_r) : \chi_i \in \widehat{k^\times}, \chi_i \neq 1, \\ \chi_i^{d_i} = 1, 且\ \chi_0 \cdots \chi_r = 1\}.$$

我们就证明了:

定理 1 方程 $a_0x_0^{n_0} + a_1x_1^{n_1} + \cdots + a_rx_r^{n_r} = 0$ 在 k^{r+1} 中的解数 N 等于

$$\begin{aligned} N &= q^r + (q-1) \\ &\quad \times \sum_{(\chi_0, \cdots, \chi_r) \in S(d_0, \cdots, d_r)} \chi_0(a_0)^{-1} \cdots \chi_r(a_r)^{-1} j(\chi_1, \cdots, \chi_r) \\ &= q^r + \frac{q-1}{q} \\ &\quad \times \sum_{\substack{(\chi_0, \cdots, \chi_r) \\ \in S(d_0, \cdots, d_r)}} \chi_0(a_0)^{-1} \cdots \chi_r(a_r)^{-1} g(\chi_0, \psi) \cdots g(\chi_r, \psi), \end{aligned}$$

其中 $d_i = \gcd(n_i, q-1)$. 特别地, N 满足下面不等式

$$|N - q^r| \leq (q-1)q^{(r-1)/2}M,$$

这里 M 是集合 $S(d_0, \cdots, d_r)$ 的势.

下面考虑非齐次方程 $a_0x_0^{n_0}+\cdots+a_rx_r^{n_r}=b$, 其中 $b\in k^\times$. 如果必要，在方程两边同除 $-b$, 这样我们总可以假定方程为

$$a_0x_0^{n_0}+a_1x_1^{n_1}+\cdots+a_rx_r^{n_r}+1=0.$$

以 N_1 表示上述方程在 k^{r+1} 中的解数，以 N' 表示方程

$$a_0x_0^{n_0}+a_1x_1^{n_1}+\cdots+a_rx_r^{n_r}+x_{r+1}^{q-1}=0$$

在 k^{r+2} 中的解数. 则由定理 1 可知

$$\begin{aligned}N'=&q^{r+1}+(q-1)\\&\times\sum_{\substack{(\chi_0,\cdots,\chi_{r+1})\\ \in S(d_0,\cdots,d_{r+1})}}\chi_0(a_0)^{-1}\cdots\chi_r(a_r)^{-1}j(\chi_1,\cdots,\chi_{r+1}),\end{aligned}$$

其中 $d_{r+1}=q-1$. 注意到 N' 与 N_1 之间的关系是

$$N'=N+(q-1)N_1,$$

这里 N 表示对应于 $x_{r+1}=0$ 的那些解的个数；而 $(q-1)N_1$ 则表示对应于 $x_{r+1}\neq 0$ 的那些解的个数，这是因为此时总有

$$x_{r+1}^{q-1}=1.$$

从而

$$\begin{aligned}N_1&=\frac{1}{q-1}(N'-N)\\&=q^r+\sum_{\substack{(\chi_0,\cdots,\chi_{r+1})\\ \in S(d_0,\cdots,d_{r+1})}}\chi_0(a_0)^{-1}\cdots\chi_r(a_r)^{-1}j(\chi_1,\cdots,\chi_{r+1})\\&\quad-\sum_{(\chi_0,\cdots,\chi_r)\in S(d_0,\cdots,d_r)}\chi_0(a_0)^{-1}\cdots\chi_r(a_r)^{-1}j(\chi_1,\cdots,\chi_r).\end{aligned}$$

在上面展开式中，我们可以视第二个和式为对应于第一个和式中 $\chi_{r+1}=1$ 的项. 这样，由 $d_{r+1}=q-1$ 知，关于 χ_{r+1} 的条件只有

$$\chi_0\chi_1\cdots\chi_{r+1}=1,$$

其中 $\chi_0,\cdots,\chi_r$ 满足 $\chi_i^{d_i}=1$ 且 $\chi_i\neq 1$. 而这样的 $(\chi_0,\cdots,\chi_r)$ 的个数等于 $(d_0-1)(d_1-1)\cdots(d_r-1)$. 从而我们证明了下述定理.

定理 2 方程 $a_0x_0^{n_0}+a_1x_1^{n_1}+\cdots+a_rx_r^{n_r}=b,\ a_i\in k^\times,\ b\in k^\times$, 在 k^{r+1} 中解的个数 N_1 满足

$$|N_1-q^r|\leq (d_0-1)(d_1-1)\cdots(d_r-1)q^{r/2},$$

其中 $d_i=\gcd(n_i,q-1)$.

在本节的最后，我们来讨论一下齐次方程的情况. 为方便起见，我们采用了一些代数几何的概念和术语，不熟悉的读者可以参阅代数几何的书籍，如参考文献 [10].

齐次方程

$$a_0x_0^m+a_1x_1^m+\cdots+a_rx_r^m=0,\qquad a_i\in k^\times$$

在 r 维射影空间 $\mathbf{P}^r(k)$ 中解的集合构成了一个射影代数簇. 我们以 $\overline{N}$ 表示该射影代数簇在 r 维射影空间 $\mathbf{P}^r(k)$ 中点的个数，则 $N=1+(q-1)\overline{N}$. 换句话说，利用定理 1, 我们有

$$\overline{N}=1+q+\cdots+q^{r-1}+\sum_{(\chi_0,\cdots,\chi_r)\in S(d,\cdots,d)}\chi_0(a_0)^{-1}\cdots\chi_r(a_r)^{-1}j(\chi_1,\cdots,\chi_r),$$

其中 $d=\gcd(m,q-1)$. 最后需要指出，今后我们研究的主要对象是射影簇，而不是前面讨论的仿射簇.

§2 Weil 猜想

对正整数 n, 以 k_n 表示 k 在一个代数闭包 $\bar{k}$ 中的 n 次域扩张. 以 $\overline{N_n}$ 表示由方程

$$a_0x_0^m+a_1x_1^m+\cdots+a_rx_r^m=0,\qquad a_i\in k^\times$$

定义的射影簇在射影空间 $\mathbf{P}^r(k_n)$ 中点的个数，记 $d(n)=\gcd(m,q^n-1)$. 由以前的讨论我们知道 $|k_n|=q^n$, 并且

$$\overline{N_n}=1+q^n+\cdots+(q^n)^{r-1}+\sum_{(\chi_0,\cdots,\chi_r)\in S_n(d(n))}\chi_0(a_0)^{-1}\cdots\chi_r(a_r)^{-1}j(\chi_1,\cdots,\chi_r),\quad(2.1)$$

其中

$$S_n(l)=\{(\chi_0,\cdots,\chi_r):\ \chi_i\in\widehat{k_n^\times},\chi_i\neq 1,\chi_i^l=1,$$
$$\text{且}\ \chi_0\cdots\chi_r=1\}.$$

显然 $S(l,\cdots,l)=S_1(l)$.

我们来研究出现于和式中的特征标. 注意到 $d=\gcd(m,q-1)$ 可整除 $d(n)$, 于是, $k^\times$ 的一个满足 $\chi^d=1$ 的特征标 χ 可诱导出一个 $k_n^\times$ 的特征标 $\mathcal{X}=\chi\circ\mathrm{N}_{k_n/k}$. 由于范映射 $\mathrm{N}_{k_n/k}$ 是满射, 故 $\mathcal{X}$ 与 χ 有同样的阶; 另一方面, 阶可以整除 d 的 $k_n^\times$ 的特征标个数正好是 d, 于是 $\widehat{k_n^\times}$ 中满足 $\chi^d=1$ 的特征标 χ 是 $k^\times$ 的特征标与范映射复合所得到的. 以后, 在不引起误会时, 我们也将 $\chi\circ\mathrm{N}_{k_n/k}$ 简记作 χ. 设 ψ 是 k 的一个非平凡加法特征标, 则对满足 $\chi_i^d=1$, $\chi_i\neq 1$, 以及 $\chi_0\cdots\chi_r=1$ 的 $k^\times$ 之特征标 $\chi_0,\chi_1,\cdots,\chi_r$, 利用第一章命题 5 可得

$$\begin{aligned}&\chi_0\circ\mathrm{N}_{k_n/k}(a_0)^{-1}\cdots\chi_r\circ\mathrm{N}_{k_n/k}(a_r)^{-1}\\&\quad\times j(\chi_1\circ\mathrm{N}_{k_n/k},\cdots,\chi_r\circ\mathrm{N}_{k_n/k})\\&\quad=(\chi_0(a_0)^{-1}\cdots\chi_r(a_r)^{-1})^n q^{-n}g(\chi_0\circ\mathrm{N}_{k_n/k},\psi\circ\mathrm{Tr}_{k_n/k})\cdots\\&\quad\times g(\chi_r\circ\mathrm{N}_{k_n/k},\psi\circ\mathrm{Tr}_{k_n/K}).\end{aligned}$$

再利用 Davenport-Hasse 等式 (第一章定理 6), 上式可简化为

$$\begin{aligned}&(\chi_0(a_0)^{-1}\cdots\chi_r(a_r)^{-1}))^n q^{-n}g(\chi_0,\psi)^n\cdots\\&\quad\times g(\chi_r,\psi)^n(-1)^{(n+1)(r+1)}\\&\quad=(\chi_0(a_0)^{-1}\cdots\chi_r(a_r)^{-1}j(\chi_1,\cdots,\chi_r))^n(-1)^{(n+1)(r+1)}.\end{aligned}$$

同样, 若 $k_n\supset k_{n'}\supset k$, 则在 (2.1) 式中, 由 $\chi_i\in\widehat{k_{n'}^\times}(i=0,1,\cdots,r)$ 生成的项等于

$$(\chi_0(a_0)^{-1}\cdots\chi_r(a_r)^{-1}j(\chi_1,\cdots,\chi_r))^{n/n'}(-1)^{(1+n/n')(r+1)}.$$

对 $(\chi_0,\cdots,\chi_r)\in\widehat{k_n^\times}$, 以 $\nu(\chi_0,\cdots,\chi_r)$ 表示使得 $\chi_0,\cdots,\chi_r$ 为 $k_m^\times$ 上的特征标与范映射 N_{k_n/k_m} 的复合的最低域扩张次数 m, 则

我们可将 (2.1) 式表示为

$$\begin{aligned}\overline{N_n} &= 1 + q^n + \cdots + q^{n(r-1)} \\ &\quad + \sum_{(\chi_0,\cdots,\chi_r)\in S_n(d(n))} (\chi_0(a_0)^{-1}\cdots\chi_r(a_r)^{-1} \\ &\quad \times j(\chi_1,\cdots,\chi_r))^{n/\nu(\chi_0,\cdots,\chi_r)}(-1)^{\left(\frac{n}{\nu(\chi_0,\cdots,\chi_r)}+1\right)(r+1)}.\end{aligned}$$

设 m' 是 m 的最大的与 q 互素的因子. 当 n 趋于 ∞ 时, 事实上只有有限多个 $d(n)$, 它们是 m' 的因子. 因此, 在结合范映射下, k 的有限扩张中, 只有有限多个乘法特征标的阶整除 m'. 令 m'' 为使得 m' 整除 $q^{m''}-1$ 之最小整数. 从而可构造形式幂级数

$$\begin{aligned}\sum_{n=1}^{\infty}\overline{N_n}U^{n-1} &= \sum_{n=1}^{r-1}\frac{q^i}{1-q^iU} \\ &\quad + (-1)^r \sum_{(\chi_0,\cdots,\chi_r)\in S_{m''}(m')} \frac{-c(\chi_0,\cdots,\chi_r)U^{\nu(\chi_0,\cdots,\chi_r)-1}}{1-c(\chi_0,\cdots,\chi_r)U^{\nu(\chi_0,\cdots,\chi_r)}},\end{aligned} \tag{2.2}$$

其中

$$\begin{aligned}c(\chi_0,\cdots,\chi_r) &= (-1)^{r+1}\chi_0(a_0)^{-1}\cdots\chi_r(a_r)^{-1}j(\chi_1,\cdots,\chi_r) \\ &= (-1)^{r+1}\chi_0(a_0)^{-1}\cdots\chi_r(a_r)^{-1}q^{-\nu} \\ &\quad \times g(\chi_0,\psi\circ\mathrm{Tr}_{k_\nu/k})\cdots g(\chi_r,\psi\circ\mathrm{Tr}_{k_\nu/k}).\end{aligned}$$

上式中的 ν 代表 $\nu(\chi_0,\cdots,\chi_r)$. 设 τ 是 $\mathrm{Gal}(k_\nu/k)$ 中的一个自同构, 则 $\chi_i^\tau=\chi_i\circ\tau$ 是一个与 χ_i 同阶的非平凡特征标, 且 $\chi_0^\tau\cdots\chi_r^\tau=1$. 我们有 $\nu(\chi_0,\cdots,\chi_r)=\nu(\chi_0^\tau,\cdots,\chi_r^\tau)$; 还有

$$\begin{aligned}g(\chi_i^\tau,\psi\circ\mathrm{Tr}_{k_\nu/k}) &= \sum_{x\in k_\nu^\times}\chi_i^\tau(x)\psi(\mathrm{Tr}_{k_\nu/k}x) \\ &= \sum_{x\in k_\nu^\times}\chi_i(x)\psi(\mathrm{Tr}_{k_\nu/k}\circ\tau^{-1}(x)) \\ &= \sum_{x\in k_\nu^\times}\chi_i(x)\psi(\mathrm{Tr}_{k_\nu/k}x) = g(\chi_i,\psi\circ\mathrm{Tr}_{k_\nu/k});\end{aligned}$$

并且对任意的 $a_i \in k^\times$ 有 $\chi_i^\tau(a_i) = \chi_i(a_i)$. 这说明：对任意的 $\tau \in \mathrm{Gal}(k_\nu/k)$, 我们有

$$c(\chi_0^\tau, \cdots, \chi_r^\tau) = c(\chi_0, \cdots, \chi_r).$$

由于对给定的 $(\chi_0, \cdots, \chi_r)$, 它有 $\nu = \nu(\chi_0, \cdots, \chi_r)$ 个共轭，而且它们有相同的 c 和 ν, 于是我们可改写 (2.2) 式为

$$\begin{aligned}\sum_{n=1}^{\infty} \overline{N_n} U^{n-1} &= \sum_{i=1}^{r-1} \frac{q^i}{1-q^i U} \\ &+ (-1)^r \sum_{(\chi_0,\cdots,\chi_r)\in \Lambda_r} \frac{-\nu(\chi_0,\cdots,\chi_r)c(\chi_0,\cdots,\chi_r)U^{\nu(\chi_0,\cdots,\chi_r)-1}}{1-c(\chi_0,\cdots,\chi_r)U^{\nu(\chi_0,\cdots,\chi_r)}},\end{aligned} \tag{2.3}$$

其中 Λ_r 是 $S_{m''}(m')$ 在 $\mathrm{Gal}(\bar{k}/k)$ 作用下的等价类. 观察上面公式，每一个商式的分子等于分母的导数的 ± 1 倍. 因此存在有理函数 $Z(U)$, 使得

$$\sum_{n=1}^{\infty} \overline{N_n} U^{n-1} = \left(\frac{\mathrm{d}}{\mathrm{d}U}\right) \log Z(U) = \frac{Z'(U)}{Z(U)}.$$

可选择 $Z(U)$ 使之是两个常数项均为 1 的多项式之商，它称为与由方程 $a_0 x_0^m + \cdots + a_r x_r^m = 0$ 定义的射影簇结合的 **zeta 函数**.

习题 1 证明：若 $\tau \in \mathrm{Gal}(k_\nu/k)$ 不是单位自同构，则

$$(\chi_0^\tau, \cdots, \chi_r^\tau) \neq (\chi_0, \cdots, \chi_r),$$

其中 $\nu = \nu(\chi_0, \cdots, \chi_r)$.

例 1 设 V_1 是由方程 $x_0^2 + x_1^2 + x_2^2 = 0$ 在有限域 k 上定义的射影簇. 假设 q 为奇数，我们有 $r = 2$ 和 $m = 2 = m'$. 注意到 $\widehat{k^\times}$ 中仅有一个 2 阶非平凡特征标 χ, 这样 χ_i 的可能选择只有 $\chi_i = \chi$, $i = 0, 1, 2$. 但此时， $\chi_0\chi_1\chi_2 = \chi^3 = \chi \neq 1$； 假设 q 为偶数，则 $m' = 1$. 于是不管何种情况， (2.3) 式中第二个和号的求和范围是空的. 从而

$$\sum_{n=1}^{\infty} \overline{N_n} U^{n-1} = \frac{1}{1-U} + \frac{q}{1-qU} = \frac{\mathrm{d}}{\mathrm{d}U} \log Z_{V_1}(U),$$

其中 $Z_{V_1}(U)=(1-U)^{-1}(1-qU)^{-1}$.

例 2 设 V_2 是由 $x_0^3+x_1^3+x_2^3=0$ 在 $\mathbf{P}^2(k)$ 中定义的射影簇，于是 $m=3$, $r=2$, $a_0=a_1=a_2=1$. 假设 $q\equiv 1(\bmod 3)$, 那么 $m'=3$ 整除 $q-1$. 我们以 $\eta,\bar{\eta}$ 表示 $k^\times$ 的 3 阶非平凡特征标. 容易验证，满足 $\chi_i^3=1$, $\chi_i\neq 1$, 以及 $\chi_0\chi_1\chi_2=1$ 的特征标组 (χ_0,χ_1,χ_2) 的仅有选择是 (η,η,η) 和 $(\bar{\eta},\bar{\eta},\bar{\eta})$. 因此，对任意 k 的非平凡加法特征标 ψ, 有

$$\nu(\eta,\eta,\eta)=\nu(\bar{\eta},\bar{\eta},\bar{\eta})=1$$

和

$$c(\eta,\eta,\eta)=-\frac{1}{q}g(\eta,\psi)^3,\quad c(\overline{\eta},\overline{\eta},\overline{\eta})=-\frac{1}{q}g(\overline{\eta},\psi)^3.$$

从而我们有

$$\begin{aligned}\sum_{n=1}^{\infty}\overline{N_n}U^{n-1}&=\frac{1}{1-U}+\frac{q}{1-qU}+\frac{\frac{1}{q}g(\eta,\psi)^3}{1+\frac{1}{q}g(\eta,\psi)^3U}+\frac{\frac{1}{q}g(\overline{\eta},\psi)^3}{1+\frac{1}{q}g(\overline{\eta},\psi)^3U}\\&=\frac{\mathrm{d}}{\mathrm{d}U}Z_{V_2}(U).\end{aligned}$$

其中

$$\begin{aligned}Z_{V_2}(U)=&\left(1+\frac{1}{q}g(\eta,\psi)^3U\right)\left(1+\frac{1}{q}g(\overline{\eta},\psi)^3U\right)\\&\times(1-U)^{-1}(1-qU)^{-1}.\end{aligned}$$

经观察发现，上面两个例子中的 zeta 函数都满足一个关于 $Z_V\left(\frac{1}{qU}\right)$ 和 $Z_V(U)$ 的函数方程. 事实上，在例 1 中，我们有

$$Z_{V_1}\left(\frac{1}{qU}\right)=\frac{1}{(qU^2)^{-1}}Z_{V_1}(U)=(qU^2)Z_{V_1}(U);$$

在例 2 中，取 $\varepsilon\in S^1$, 使得 $g(\eta,\psi)=\varepsilon\sqrt{q}$. 注意到

$$\eta(-1)=\eta(-1)^3=1,$$

所以 $g(\overline{\eta},\psi)=\eta(-1)\overline{\varepsilon}\sqrt{q}=\overline{\varepsilon}\sqrt{q}$. 于是我们有

$$Z_{V_2}(U)=\frac{(1+\varepsilon^3\sqrt{q}U)(1+\bar{\varepsilon}^3\sqrt{q}U)}{(1-U)(1-qU)},$$

且

$$Z_{V_2}\left(\frac{1}{qU}\right)=\frac{(\sqrt{q}U)^{-2}(\sqrt{q}U+\varepsilon^3)(\sqrt{q}U+\bar{\varepsilon}^3)}{(qU^2)^{-1}(1-U)(1-qU)}$$
$$=\frac{(1+\varepsilon^3\sqrt{q}U)(1+\bar{\varepsilon}^3\sqrt{q}U)}{(1-U)(1-qU)}=Z_{V_2}(U).$$

现在我们来讨论由方程 $a_0x_0^m+a_1x_1^m+\cdots+a_rx_r^m=0$ 定义的射影簇 V 所结合的 zeta 函数 $Z_V(U)$. 由 (2.3) 式可以看出

$$Z_V(U)=\prod_{i=0}^{r-1}(1-q^iU)^{-1}$$
$$\times\prod_{(\chi_0,\cdots,\chi_r)\in\Lambda_r}(1-c(\chi_0,\cdots,\chi_r)U^{\nu(\chi_0,\cdots,\chi_r)})^{(-1)^r}.$$

此处我们应注意, 若 $(\chi_0,\cdots,\chi_r)$ 出现于上面的乘积中, 则 $(\overline{\chi_0},\cdots,\overline{\chi_r})$ 也出现于这个乘积之中, 并且

$$\nu(\overline{\chi_0},\cdots,\overline{\chi_r})=\nu(\chi_0,\cdots,\chi_r)\qquad(\text{ 记为}\nu)$$

及

$$c(\overline{\chi_0},\cdots,\overline{\chi_r})=(-1)^{r+1}\overline{\chi_0}(a_0)^{-1}\cdots\overline{\chi_r}(a_r)^{-1}j(\overline{\chi_1},\cdots,\overline{\chi_r})$$
$$=(-1)^{r+1}\chi_0(a_0)\cdots\chi_r(a_r)\overline{j(\chi_1,\cdots,\chi_r)}$$
$$=\overline{c(\chi_0,\cdots,\chi_r)}.$$

由第一章命题 5 知, $j(\chi_1,\cdots,\chi_r)$ 的绝对值是 $q^{\nu(r-1)/2}$, 于是我们可记

$$c(\chi_0,\cdots,\chi_r)=\varepsilon(\chi_0,\cdots,\chi_r)q^{\nu(r-1)/2},$$

其中 $\varepsilon(\chi_0,\cdots,\chi_r)\in S^1$. 由此看出

$$\begin{aligned}1-c(\chi_0,\cdots,\chi_r)\left(\frac{1}{q^{r-1}U}\right)^{\nu} &= -(q^{(r-1)/2}U)^{-\nu}\varepsilon(\chi_0,\cdots,\chi_r)\\ &\quad\times(1-\overline{\varepsilon(\chi_0,\cdots,\chi_r)}q^{\nu(r-1)/2}U^{\nu})\\ &= -(q^{(r-1)/2}U)^{-\nu}\varepsilon(\chi_0,\cdots,\chi_r)(1-c(\overline{\chi_0},\cdots,\overline{\chi_r})U^{\nu}).\end{aligned}$$

若 $(\overline{\chi_0},\cdots,\overline{\chi_r})$ 不与 $(\chi_0,\cdots,\chi_r)$ Galois 共轭, 则

$$\varepsilon(\overline{\chi_0},\cdots,\overline{\chi_r})\varepsilon(\chi_0,\cdots,\chi_r)=1,$$

否则 $\varepsilon(\chi_0,\cdots,\chi_r)=\pm1$. 这就证明了:

$$\begin{aligned}Z_V\left(\frac{1}{q^{r-1}}U\right) &= \prod_{i=0}^{r-1}(-1)^r q^{r(r-1)/2}U^r\prod_{i=0}^{r-1}(1-q^iU)^{-1}\\ &\quad\times\prod_{(\chi_0,\cdots,\chi_r)\in\Lambda_r}[-\varepsilon(\chi_0,\cdots,\chi_r)^{(-1)^r}\\ &\quad\times(q^{(r-1)/2}U)^{(-1)^{r+1}\nu(\chi_0,\cdots,\chi_r)}\\ &\quad\times(1-c(\overline{\chi_0},\cdots,\overline{\chi_r})U^{\nu(\overline{\chi_0},\cdots,\overline{\chi_r})})^{(-1)^r}]\\ &= \pm(q^{(r-1)/2}U)^e Z_V(U),\end{aligned}$$

其中指数 e 是 Z_V 的极点个数减去其零点个数, 而 $r-1$ 为簇 V 的维数.

从上面的计算和对曲线研究的结果, A. Weil 对非奇异不可约射影簇提出了下面影响深远的猜想, 它揭示了有限域上代数簇的算术与复数域上代数簇的拓扑之间深刻的联系.

设 V 是一个定义在有限域 k 上的维数为 d 的不可约射影簇. 以 N_n 表示 V 在 k 的 n 次域扩张上点的个数, 结合 V 的 zeta 函数定义为:

$$Z_V(U)=\exp\left(\sum_{n=1}^{\infty}\overline{N_n}\frac{U^n}{n}\right).$$

这是 U 的一个有有理系数的形式幂级数. 1949 年, A. Weil[14] 提出了关于 Z_V 的下面四个猜测:

(I) **有理性** $Z_V(U)$ 是 U 的系数为有理数的有理函数.

(II) **函数方程** 存在一个整数 E, 称为簇 V 的 **Euler-Poincaré 示性数**, 使得 Z_V 满足函数方程

$$Z_V\left(\frac{1}{q^dU}\right) = \pm(q^{d/2}U)^E Z_V(U).$$

(III) **Riemann 猜想** 存在 $2d+1$ 个整系数多项式 $P_0(U)$, $P_1(U), \cdots, P_{2d}(U)$, 其中 $P_0(U) = 1-U$ 和 $P_{2d}(U) = 1-q^dU$, 使得

$$Z_V(U) = \frac{P_1(U)P_3(U)\cdots P_{2d-1}(U)}{P_0(U)P_2(U)\cdots P_{2d}(U)};$$

更进一步, 每个 $P_i(U)$ 均可写作

$$P_i(U) = \prod_{j=1}^{B_i}(1-\alpha_{ij}U),$$

其中 α_{ij} 是代数整数, 其绝对值 $|\alpha_{ij}| = q^{i/2}$. (注意, 如果 P_i 存在, 这些条件唯一确定这一多项式.)

(IV) **Betti 数** 我们称多项式 P_i 的次数 B_i 为簇 V 的第 i 个 **Betti 数**. 则出现于函数方程中的 V 的 Euler-Poincaré 示性数 E 等于 $\sum_{i=0}^{2d}(-1)^iB_i$. 若 V 是一个由定义在一个数域的整数环上的簇 $\widetilde{V}$ 通过模一个素理想约化而得到的簇, 则 B_i 等于上同调群 $H^i(\widetilde{V_h},\mathbf{Z})$ 的阶, 其中 $\widetilde{V_h}$ 是由同样方程定义的, 具有通常拓扑的复射影簇.

例 1 中的簇 V_1 是 $\mathbf{P}^2$ 中的射影直线, 它的亏格是 0, 其 Euler-Poincaré 示性数 $E=1-0+1=2$, 且 (I) ~ (IV) 都满足 (请读者自己验证). 例 2 中的簇 V_2 在 k 的特征 char $k \neq 2,3$ 时是一条椭圆曲线, 即一条亏格为 1 的射影曲线. 我们发现它的 Euler-Poincaré 示性数 $E=0=1-2+1$, 且 (I) ~ (IV) 也成立. 对一般有限域上

非奇异射影曲线的 zeta 函数的概念是 1931 年由 F. K. Schmidt 首先引入的. 他证明了对一条定义在有 q 个元素的有限域上的亏格为 g 的非奇异射影曲线 C, 其 zeta 函数有下面形式

$$Z_C(U) = \frac{P_1(U)}{(1-U)(1-qU)},$$

其中 $P_1(U)$ 是一个有理系数的 $2g$ 阶多项式, 其常数项为 1, 且 Z_C 满足函数方程

$$Z_C\left(\frac{1}{qU}\right) = \pm(qU^2)^{1-g}Z_C(U).$$

关于曲线 C 上的 Riemann 猜想, 即 $P_1(U)$ 的零点有绝对值 $q^{1/2}$, 是首先由 E. Artin 所猜测的. 他还对一些特殊的射影曲线给予了证明. 曲线亏格 $g=1$ 的情况, 则是由 H. Hasse[11] 证明的. 而 A. Weil[15] 在 1940 年对任意亏格的情况给予了证明.

由方程 $a_0x_0^m + \cdots + a_rx_r^m = 0$ 所定义的 Fermat 超曲面 V 有维数 $d = r-1$. 在 r 为偶数, 亦即 d 为奇数时, 有

$$P_{2i}(U) = 1 - q^iU, \quad 0 \le i \le d.$$

而对 0 与 $2d$ 之间的奇数 i, 除了

$$P_d(U) = \prod_{(\chi_0,\cdots,\chi_r)\in\Lambda_r} (1 - c(\chi_0,\cdots,\chi_r)U^{\nu(\chi_0,\cdots,\chi_r)})$$

之外, 均有 $P_i(U) = 1$; 当 r 为奇数, d 为偶数时, 我们有

$$P_{2i}(U) = 1 - q^iU, \quad 0 \le i \le d,\ 2i \ne d,$$

和

$$P_d(U) = (1 - q^{d/2}U) \prod_{(\chi_0,\cdots,\chi_r)\in\Lambda_r} (1 - c(\chi_0,\cdots,\chi_r)U^{\nu(\chi_0,\cdots,\chi_r)}),$$

其他 $P_i(U)$ 均为 1.

因此, 不管何种情况, zeta 函数 Z_V 都满足 Weil 猜想.

习题 2 令 C 为一条定义在有限域 k 上的亏格为 g 的非奇异射影曲线，证明 C 上的 Riemann 猜想等价于

$$|\overline{N_n} - q^n - 1| \leq 2gq^{n/2}, \qquad n \geq 1.$$

这里 $\overline{N_n}$ 与过去一样，都表示曲线 C 在 k 的 n 次域扩张 k_n 中点的个数.

习题 3 设 $V = \mathbf{P}^d(k)$. 由定义出发，检验它的 zeta 函数等于

$$Z_V(U) = \frac{1}{(1-U)(1-qU)\cdots(1-q^dU)}.$$

进一步，证明 Weil 猜想对 $V = \mathbf{P}^d(k)$ 成立.

习题 4 确定由方程 $x_0^3 + x_1^3 + x_2^3 = 0$ 定义的有限域 k 上的射影簇 V 的 zeta 函数，其中 $|k| = q \equiv 2(\bmod 3)$, q 为奇数. 进而验证关于 Z_V 的 Weil 猜想.

C. Gauss 最早开始研究一个整系数多项式模 p 的解数 N_p. 特别地，他希望知道 N_p 是如何随着 p 变化. 假设多项式定义了一个 d 维不可约非奇异射影簇，则 Weil 猜想导出

$$|N_p - (1 + p + \cdots + p^d)| \leq bp^{d/2},$$

其中 b 是由同一个多项式在 $\mathbf{C}$ 上定义的相伴射影簇的第 d 个 Betti 数.

§3 Weil 猜想的上同调解释

正如 A. Weil 本人所指出的：如果能模拟复数域 $\mathbf{C}$ 上簇的上同调理论，对抽象簇建立合适的上同调理论，那么从上同调理论的标准性质就可能导出 Weil 猜想. B. Dwork 利用 p-adic 分析成功地证明了 zeta 函数的有理性和函数方程. 大多数关于 Weil 猜想的其他工作是寻找一种好的上同调理论，它既能给出猜想 (IV) 中的 Betti 数，并且该上同调的系数是在一个特征为 0 的域中，使得有相应的 Lefschetz 不动点定理成立. 这个想法曾有许多人尝试过.

1963 年，A. Grothendieck 利用代数簇的平展拓扑发展了抽象代数簇的 l-adic 上同调理论，由此他得到了 zeta 函数的有理性及函数方程的另一个证明. 猜想的最深刻部分是 Riemann 猜想，它是被 P. Deligne 在 1973 年利用 l-adic 上同调成功地给予了证明.

在这一节中，我们将简单解释 l-adic 上同调与 Weil 猜想之间的联系. 由于这些内容涉及代数几何学极深刻的部分，限于本书的目的和篇幅，我们将不给出所有概念的定义和解释. 请有兴趣的读者参阅有关文献.

在本节中，V 表示一个定义在有限域 k 上的 d 维非奇异的不可约射影簇，$\overline{V}$ 表示 V 在 k 的一个代数闭包 $\bar{k}$ 上的点集，又设 l 是一个不能整除 q 的素数. 在 V 上赋以平展拓扑，则对每个自然数 r, 有一个平展上同调 $H_{et}^i(\overline{V}, \mathbf{Z}/l^r\mathbf{Z})$. V 的 l-adic 上同调定义为

$$H^i(\overline{V}, \mathbf{Q}_l) = \left(\lim_{\overleftarrow{r}} H_{et}^i(\overline{V}, \mathbf{Z}/l^r\mathbf{Z})\right) \bigotimes_{\mathbf{Z}_l} \mathbf{Q}_l\,,$$

其中 $\mathbf{Z}_l$ 是 l-adic 整数环，即

$$\mathbf{Z}_l = \left\{ \sum_{n=0}^{\infty} a_n l^n : 0 \le a_n \le l-1 \right\}.$$

它是 $\mathbf{Z}/l^r\mathbf{Z}$ 在 r 趋于 ∞ 时的反极限； $\mathbf{Q}_l$ 是 $\mathbf{Z}_l$ 的商域，亦可视为 $\mathbf{Q}$ 关于 $\mathbf{Q}$ 上的 l-adic 度量的完备化. l-adic 上同调有下面一些性质:

(1) $H^i(\overline{V}, \mathbf{Q}_l)$ 是 $\mathbf{Q}_l$ 上的有限维向量空间, 且除了当 $0 \le i \le 2d$ 时外，其余情况均为 0.

(2) 对所有的 i 和 j, 有一个上积 (cup product) 结构:

$$H^i(\overline{V}, \mathbf{Q}_l) \times H^j(\overline{V}, \mathbf{Q}_l) \longrightarrow H^{i+j}(\overline{V}, \mathbf{Q}_l).$$

(3) **Poincaré 对偶** 顶上同调群 $H^{2d}(\overline{V}, \mathbf{Q}_l)$ 是一维的, 当 $0 \le i \le 2d$ 时，上积定义了一个非退化配对 (pairing):

$$H^i(\overline{V}, \mathbf{Q}_l) \times H^{2d-i}(\overline{V}, \mathbf{Q}_l) \longrightarrow H^{2d}(\overline{V}, \mathbf{Q}_l) \cong \mathbf{Q}_l.$$

(4) **Künneth 公式** 对两个非奇异簇 X 和 Y, 有一个分次代数的自然同构:

$$H^*(X,\mathbf{Q}_l)\otimes H^*(Y,\mathbf{Q}_l)\xrightarrow{\sim}H^*(X\times Y,\mathbf{Q}_l).$$

(5) **Lefschetz 不动点公式** 设 $f:\overline{V}\longrightarrow\overline{V}$ 是一个有孤立不动点的态射, 每个不动点的重数为 1, 即 f 在 $\overline{V}\times\overline{V}$ 中的图形与 $\overline{V}\times\overline{V}$ 的对角线横截地相交, 以 $L(f,\overline{V})$ 表示 f 的不动点数 (由于 $\overline{V}$ 是紧的, 故 $L(f,\overline{V})$ 是有限的), 此数可表为

$$L(f,\overline{V})=\sum_{i=0}^{2d}(-1)^i\mathrm{Tr}(f^{(i)};H^i(\overline{V},\mathbf{Q}_l)),$$

其中 $f^{(i)}$ 是 f 在 H^i 上诱导的拉回 (pull-back) 映射.

(6) **比较定理** 若 V 是一个定义在一个数域的整数环上的非奇异射影簇 $\widetilde{V}$ 通过模一个素理想约化而得到的簇, 则

$$H^i(\overline{V},\mathbf{Q}_l)\otimes_{\mathbf{Q}_l}\mathbf{C}\cong H^i(\widetilde{V_h},\mathbf{C}),$$

其中 $\widetilde{V_h}$ 是具有传统拓扑的相伴复簇.

(7) **闭链的上同调类** 设 Z 是一个余维数为 i 的子簇, 则 Z 对应有一个相伴的上同调类 $\eta(Z)\in H^{2i}(\overline{V},\mathbf{Q}_l)$, 这里 $\overline{V}$ 与 (6) 中的 V 相同. 这个对应被线性地扩展为一个闭链. 有理等价的闭链有同样的上同调类, 闭链的交是上同调类的上积. 进一步, 若 P 是 V 的一个闭点, 则 $\eta(P)\in H^{2d}(\overline{V},\mathbf{Q}_l)$ 是非 0 的.

以上诸性质可以通过定义在 $\mathbf{C}$ 上的不可约非奇异射影簇的上同调理论来理解. 它们主要是由 W. V. D. Hodge 和 S. Lefschetz 所发展的.

现在我们来讨论上述性质的一些推论. 注意到 Frobenius 态射 $\phi:\overline{V}\longrightarrow\overline{V}$ 将点 (a_i) 映为 (a_i^q). 于是对 $\overline{V}$ 中的每个点, 其坐标都在 k_n 中的充要条件是它是 ϕ^n 的不动点, 因此

$$\overline{N_n}=\phi^n\text{ 的不动点数 }=L(\phi^n,V).$$

由于 V 是非奇异的，故可以用上述性质 (5)——Lefschetz 不动点公式来计算 $\overline{N_n}$，即

$$\overline{N_n} = \sum_{i=0}^{2d} (-1)^i \mathrm{Tr}((\phi^n)^{(i)}; H^i(\overline{V}, \mathbf{Q}_l)).$$

将此代入 V 的相伴 zeta 函数的定义，我们得到

$$\begin{aligned} Z_V(U) &= \prod_{i=0}^{2d} \left[\exp \left(\sum_{n=1}^{\infty} \mathrm{Tr}((\phi^n)^{(i)}; H^i(\overline{V}, \mathbf{Q}_l)) \frac{U^n}{n} \right) \right]^{(-1)^i} \\ &= \prod_{i=0}^{2d} \left[\exp \left(\sum_{n=1}^{\infty} \mathrm{Tr}((\phi^{(i)})^n; H^i(\overline{V}, \mathbf{Q}_l)) \frac{U^n}{n} \right) \right]^{(-1)^i}. \end{aligned}$$

对每个 i，我们都可用下面这个线性代数的结果来估计指数部分.

引理 1 设 f 是一个定义在特征为 0 的域 K 上的有限维线性空间 W 的自同态，则作为系数在 K 中 U 的形式幂级数，有

$$\exp\left(\sum_{n=1}^{\infty} \mathrm{Tr}(f^n; W) \frac{U^n}{n} \right) = \det(1 - fU; W)^{-1}. \tag{3.1}$$

证 若 W 是 1 维的，则 f 的是乘上一个常量 λ 的映射，故而

$$\begin{aligned} \exp\left(\sum_{n=1}^{\infty} \mathrm{Tr}(f^n, W) \frac{U^n}{n} \right) &= \exp\left(\sum_{n=1}^{\infty} \lambda^n \frac{U^n}{n} \right) \\ &= \frac{1}{1 - \lambda U} = \det(1 - \lambda U; W)^{-1}. \end{aligned}$$

证明一般情况的方法是对 W 的维数进行归纳. 我们不妨设 K 是代数闭的，这使得 f 有一个特征向量，它生成出 W 的一个 1 维不变子空间 W'，由此得到一个短正合列

$$0 \longrightarrow W' \longrightarrow W \longrightarrow W/W' \longrightarrow 0.$$

从而

$$\exp\left(\sum_{n=1}^{\infty} \mathrm{Tr}(f^n, W') \frac{U^n}{n} \right) \quad 与 \quad \exp\left(\sum_{n=1}^{\infty} \mathrm{Tr}(f^n, W/W') \frac{U^n}{n} \right)$$

的积正好为 (3.1) 式的左边，而

$$\det(1-fU;W') \quad 与 \quad \det(1-fU;W/W')$$

的积恰好是 (3.1) 式的右边. 又由归纳假设知，(3.1) 式对于 W' 和 W/W' 都成立，从而得到所需结论.

由引理 1 立即就可导出下述定理.

定理 3 *设 V 是一个定义在 k 上的维数为 d 的非奇异不可约射影簇. V 的相伴 zeta 函数 $Z_V(U)$ 有下面表示形式*

$$Z_V(U)=\frac{P_1(U)P_3(U)\cdots P_{2d-1}(U)}{P_0(U)P_2(U)\cdots P_{2d}(U)},$$

其中 $P_i(U)=\det(1-\phi^{(i)}U;H^i(V,\mathbf{Q}_l))$, 这里 $\phi^{(i)}$ 是 Frobenius 态射 $\phi:\overline{V}\longrightarrow\overline{V}$ 在 $H^i(V,\mathbf{Q}_l)$ 上诱导的映射.

我们知道，$Z_V(U)$ 是 U 的有理系数的形式幂级数，上面定理说明它也是一个系数在 $\mathbf{Q}_l$ 中的 U 的有理函数，于是它是一个系数在 $\mathbf{Q}$ 中的 U 的有理函数，然而这并不意味着每个 $P_i(U)$ 也是有理系数的. 同样，定理 3 中的 P_i 也不知道是不是猜想 (III) 中所说的 P_i. 另一方面，由于 ϕ_0 作用在 $H^0(\overline{V},\mathbf{Q}_l)$ 上如同单位映射，故 $P_0(U)=1-U$. 进一步，由于 Frobenius 态射是一个次数为 q^d 的态射，它在上同调群 $H^{2d}(\overline{V},\mathbf{Q}_l)$ 上诱导了一个乘以 q^d 的乘法映射，于是 $P_{2d}(U)=1-q^dU$. 设

$$B_i=\deg P_i=\dim H^i(\overline{V},\mathbf{Q}_l),$$

此时，也同样无法肯定 B_i 就是猜想中的 Betti 数.

下面我们将看到猜想 (II)(函数方程) 可以由性质 (3)——Poincaré 对偶导出. 事实上，对任意的

$$v\in H^i(\overline{V},\mathbf{Q}_l) \quad 和 \quad w\in H^{2d-i}(\overline{V},\mathbf{Q}_l),$$

由

$$H^i(\overline{V},\mathbf{Q}_l)\times H^{2d-i}(\overline{V},\mathbf{Q}_l)\longrightarrow H^{2d}(\overline{V},\mathbf{Q}_l)$$

的上积同态将 $(\phi^{(i)}(v), \phi^{(2d-i)}(w))$ 映为

$$\phi^{(i)}(v) \vee \phi^{(2d-i)}(w) = \phi^{(2d)}(v \vee w) = q^d(v \vee w).$$

引理 2 设 A,B 是域 K 上维数 r 的向量空间，并有一个完全配对 $\langle , \rangle : A \times B \longrightarrow K$. 假设 f,g 分别为 A,B 上的自同态，使得存在一个非零元 $\lambda \in K$, 满足

$$\langle fa, gb \rangle = \lambda \langle a,b \rangle, \quad a \in A,\ b \in B.$$

则 f 和 g 都是可逆的，且，${}^t gf = \lambda I_r$ (这里将 g,f 视作 $r \times r$ 矩阵，I_r 是 $r \times r$ 单位矩阵). 于是

$$\det(1 - gU; B) = \frac{(-\lambda U)^r}{\det(f; A)} \det\left(1 - \frac{1}{\lambda U} f; A\right)$$

和

$$\det(f; A)\det(g; B) = \lambda^r.$$

(证明是初等的，留给读者作为练习.)

利用上面这个线性代数的结果我们可以导出

$$\begin{aligned} P_{2d-i}(U) &= \det(1 - \phi^{(2d-i)}U; H^{2d-i}(\overline{V}, \mathbf{Q}_l)) \\ &= \frac{(-1)^{B_i}(q^dU)^{B_i}}{\det(\phi^{(i)}; H^i(\overline{V}, \mathbf{Q}_l))} \det\left(1 - \frac{1}{q^dU}\phi^{(i)}; H^i(\overline{V}, \mathbf{Q}_l)\right) \\ &= \frac{(-q^dU)^{B_i}}{\det(\phi^{(i)}; H^i(\overline{V}, \mathbf{Q}_l))} P_i\left(\frac{1}{q^dU}\right) \end{aligned}$$

以及

$$\det(\phi^{(i)}; H^i(\overline{V}, \mathbf{Q}_l))\det(\phi^{(2d-i)}; H^{2d-i}(\overline{V}, \mathbf{Q}_l)) = q^{dB_i}.$$

其实 $q^{-(2d-i)/2}\phi^{(2d-i)}$ 的转置是 $q^{-i/2}\phi^{(i)}$ 的逆. 于是结合定理 3 就导出了猜想 (II)(函数方程), 其中

$$E = \sum_{i=0}^{2d} (-1)^i B_i .$$

上面讨论已经从形式上证明了猜想 (I), (II) 和 (IV) 可以由 l-adic 上同调的性质得到，同时定理 3 也给出了 zeta 函数的解释. 事实上，定理 3 中的 P_i 和 B_i 就是猜想所言的 P_i 和 B_i. Riemann 猜想 (III) 的正确性是由 P. Deligne 在 1973 年证明的，他用到了 l-adic 上同调更深刻的性质.

定理 4(Deligne[1]) 定理 3 中多项式 $P_i(U)$ 有独立于 l 的整系数，且它们可以写作

$$P_i(U) = \prod_{j=1}^{B_i} (1 - \alpha_{ij} U) ,$$

其中 α_{ij} 是绝对值为 $q^{i/2}$ 的代数整数.

在这里我们将不准备谈论 P. Deligne 的证明 (有兴趣的读者可参阅 N. Katz[13]), 但我们将简单解释一下它为什么是对的. 人们可以找到存在一个余维数为 1 的闭链 Z, 使得 $h = \eta(Z)$ 是一个 $H^2(\overline{V}, \mathbf{Q}_l)$ 中的非平凡类，且 $\phi^{(2)}(h) = qh$, 则与 h 作 $d-i$ 次上积可导出一个从 $H^i(\overline{V}, \mathbf{Q}_l)$ 到 $H^{i+2(d-i)}(\overline{V}, \mathbf{Q}_l) = H^{2d-i}(\overline{V}, \mathbf{Q}_l)$ 的同构，这连同 Poincaré 对偶就给出一个从 $H^i(\overline{V}, \mathbf{Q}_l) \times H^i(\overline{V}, \mathbf{Q}_l)$ 到 $H^{2d}(\overline{V}, \mathbf{Q}_l)$ 的非退化配对. 当 V 有一个相伴的非奇异不可约射影簇 $\widetilde{V_h}$ 时，这也是从 $H^i(\widetilde{V_h}, \mathbf{C}) \times H^i(\widetilde{V_h}, \mathbf{C})$ 到 $H^{2d}(\widetilde{V_h}, \mathbf{C})$ 的非退化配对. 当 i 是偶数时， $H^i(\widetilde{V_h}, \mathbf{C})$ 包含一个 $\mathbf{R}$ 上 B_i 维的，且在 $\phi^{(i)}$ 作用下不变的实子空间 $A^i(\widetilde{V_h})$, 使得在 $A^i(\widetilde{V_h})$ 中，前述配对是一个非退化内积，且 $q^{-i/2}\phi^{(i)}$ 关于这个配对是一个酉映射. 这表明，在 i 是偶数时， $\phi^{(i)}$ 的特征值有所述的绝对值 $q^{i/2}$. 当 i 是奇数时，我们研究 $\overline{V} \times \overline{V}$. 此时， $\phi^{(i)}$ 在 $H^i(\overline{V}, \mathbf{Q}_l)$ 上特征值之大小可以由在 $H^{2i}(\overline{V} \times \overline{V}, \mathbf{Q}_l)$ 上诱导的 Frobenius 态射得出.

注 如前所证, $\phi^{(i)}$ 在 $H^i(\overline{V}, \mathbf{Q}_l)$ 上的特征值就是出现于 $P_i(U) = \prod_{j=1}^{B_i} (1 - \alpha_{ij} U)$ 中的 α_{ij}. 特别地， $\phi^{(i)}$ 的特征值有绝对值 $q^{i/2}$.

§4 zeta 函数的 Euler 积

设 K 是一个域, $P(T_1,\cdots,T_r)$ 是 $K[T_1,\cdots,T_r]$ 中一个不可约多项式, P 在 K^r 中的解的集合称为**仿射代数超平面**. 我们也将考虑多项式 P 在 K 的任意有限代数扩张中的解. 以 $\overline{K}$ 表 K 的一个代数闭包, V 为多项式 P 在 $\overline{K}^r$ 中解的集合. 给定 V 中一点 $x=(x_1,\cdots,x_r)$, 以 $K(x)$ 表示由 x 的坐标生成的域 $K(x_1,\cdots,x_r)$, 这是 K 的一个有限扩张, 其在 K 上的次数称为 x 的次数, 记为 $\deg x$. 考虑将 T_i 映为 x_i 的由 $K[T_1,\cdots,T_r]$ 到 K 的同态, 其核 m 是 $K[T_1,\cdots,T_r]$ 中包含多项式 P 的极大理想. 商域 $K[T_1,\cdots,T_r]/\mathrm{m}$ 同构于 $K(x)$. 定义 $\deg\mathrm{m}=\deg x$. 在 K 上有 $\deg x=[K(x):K]$ 个从 $K(x)$ 到 $\overline{K}$ 中的 K-嵌入. 对每个嵌入 σ, 点 $x^\sigma=(x_1^\sigma,\cdots,x_r^\sigma)$ 也在 V 中, 且从 $K[T_1,\cdots,T_r]$ 到 $\overline{K}$ 的映 T_i 为 x_i^σ 的同态也有核 m, 这是由于 m 中的多项式系数均在 K 中. 因此, 理想 m 对应 V 中 $\deg\mathrm{m}$ 个点; 反过来, 给出一个包含 P 的极大理想 m, 它也对应了 V 中 $\deg\mathrm{m}$ 个点. x 在 $K(x)$ 到 $\overline{K}$ 中所有 K-嵌入下的轨道, 即 $\{x^\sigma:\sigma\in\mathrm{Gal}(\overline{K}/K)\}$ 称为 V 的一个 **闭点**, 它可由一个极大理想表示.

当 $K=k$ 是一个有限域时, V 的 zeta 函数定义为

$$Z_V(U)=\prod_{\substack{\mathrm{m}\ \text{为极大理想}\\ P\in\mathrm{m}}}(1-U^{\deg\mathrm{m}})^{-1}$$

$$=\prod_{x\ \text{为}\ V\ \text{中闭点}}(1-U^{\deg x})^{-1}.$$

注意到, V 中位于 k_n^r 中的点是那些次数可整除 n 的点 x, 于是至多有 q^{nr} 个极大理想 m 使得 $P\in\mathrm{m}$ 且 $\deg\mathrm{m}$ 整除 n. 这表明, 当 U 足够小时, 无限乘积是绝对收敛的. 进一步, 对充分小的 U, 我

们有

$$\frac{Z_V(U)'}{Z_V(U)} = \sum_{\mathfrak{m}} \frac{\deg \mathfrak{m} \cdot U^{\deg \mathfrak{m}-1}}{1-U^{\deg \mathfrak{m}}}$$

$$= \sum_{l=1}^{\infty} \sum_{\mathfrak{m}} \deg \mathfrak{m} \cdot U^{l \deg \mathfrak{m}-1} = \sum_{v=1}^{\infty} N_v U^{v-1},$$

其中关于 $\mathfrak{m}$ 的求和是通过所有包含 P 的极大理想,

$$N_v = \sum_{\deg \mathfrak{m} | v} \deg \mathfrak{m}$$

是 V 在 k_v^r 中点的个数.

一般地, 若 V 是一个定义在有限域上的非奇异射影簇, 则它是几个仿射簇的并. 在 §2 中用在域的有限扩张上的解数定义的 zeta 函数 $Z_V(U)$ 有 Euler 积

$$Z_V(U) = \exp\left(\sum_{n=1}^{\infty} \overline{N_n} \frac{U^n}{n}\right) = \prod_{x \text{ 为 } V \text{ 中闭点}} (1-U^{\deg x})^{-1}.$$

例 3 设 C 是一条定义在有限域 k 上的射影直线, 它有一个 "无穷远点", 剩下的点则在 k 上的一条仿射直线上. 在仿射直线上的点可被 $k[T]$ 中的首一不可约多项式或 $k[T]$ 的极大理想所刻画, 从而可得

$$Z_C(U) = (1-U)^{-1} \prod_{\substack{f \in k[T] \\ f:\text{ 首一, 不可约}}} (1-U^{\deg f})^{-1}.$$

例 4 设 C 是一条由 k 上齐次多项式 $P(T_0, T_1, T_2)$ 定义的非奇异射影曲线. 那么 P 在 $\{(x_0 : x_1 : x2) : x_0 \neq 0\}$ 中的解可等同于由

$$P(T, Y) = P(1, T_1/T_0, T_2/T_0)$$

定义的仿射曲线 C 上的点, 其中 $T = T_1/T_0$, $Y = T_2/T_0$. 我们不妨假设 P 关于 Y 是首一的. 以 F 表示域 $k(T)$, 以 K 表示域

$F[Y]/(P(T,Y))$. 这是域 F 的一个有限扩张, 称为 C 的 **有理函数域**. 设 $\mathcal{O}$ 为 $k[T]$ 在 K 中的整闭包, $k[T,Y]$ 中包含多项式 P 的极大理想 $\mathfrak{m}$ 对应了 $\mathcal{O}$ 的极大理想 $\mathfrak{p}$. 进一步, 若 $\mathfrak{p}$ 对应 C 上闭点 x, 则 $\mathcal{O}/\mathfrak{p}$ 同构于 $k(x)$, 我们称之为 $\mathfrak{p}$ 的 **剩余类域**. 定义

$$\deg \mathfrak{p} = \deg x = [\mathcal{O}/\mathfrak{p} : k].$$

于是剩余类域 $\mathcal{O}/\mathfrak{p}$ 的势是 $q^{\deg \mathfrak{p}}$, 这也称作 $\mathfrak{p}$ 的范 $N\mathfrak{p}$. 结合仿射曲线 C 的 zeta 函数是

$$Z_C(U) = \prod_{\mathfrak{p}:\mathcal{O}\text{中极大理想}} (1 - U^{\deg \mathfrak{p}})^{-1}.$$

我们称这些极大理想 $\mathfrak{p}$ 为 C 或 K 的 **有限位**.

在 $\bar{C}\setminus C$ 中的点是多项式 P 在 $\{(x_0,x_1,x_2):x_0=0\}$ 中的解. 它们可视为我们关于仿射子簇选取的无穷远点, 这样的点共有有限多个, 它们可由 $k\left[\frac{1}{T}\right]$ 在 K 中整闭包 $\mathcal{O}'$ 内包含 $\frac{1}{T}$ 的极大理想 $\mathfrak{p}_\infty$ 来表示, 这些称为 C 或 K 的 **无限位**. 同样地, $\deg \mathfrak{p}_\infty$ 定义为 $[\mathcal{O}'/\mathfrak{p}_\infty : k]$, $N\mathfrak{p}_\infty$ 恰等于剩余类域 $\mathcal{O}'/\mathfrak{p}_\infty$ 的势, 即 $q^{\deg \mathfrak{p}_\infty}$.

有限位与无限位合在一起表达了 C 上所有闭点, 从而我们有

$$Z_{\bar{C}}(U) = \prod_{\mathfrak{p}:\ K\text{ 中的位}} (1 - U^{\deg \mathfrak{p}})^{-1}.$$

域 $F = k(T)$ 称为 k 上 **单变量有理函数域**. 函数域 K 是 F 的有限扩张. 设 k_v 是 k 包含在 K 中的最大代数扩张, 我们称 k_v 为 K 的 **常数域**. 函数域 K 是一个定义在 k_v 上的一条非奇异射影曲线上的有理函数域.

参 考 文 献

[1] P. Deligne, *La conjecture de Weil I*, Publ. Math. IHES, **43**(1974), 273~307.

[2] P. Deligne . *La conjecture de Weil II*, Publ. Math. IHES, **52**(1974), 137~252.

[3] J. A. Dieudonné, *On the history of the Weil conjectures*, The Mathematical Intelligencer 10, Springer-Verlag, Berlin , 1975.

[4] B. Dwork, *On the rationality of the zeta function of an algebraic variety*, Amer. J. Math., **82**(1960), 631~648.

[5] E. Freitag and R. Kiehl, *Etale Cohomology and the Weil Conjecture*, Springer-Verlag, Berlin , 1988.

[6] A. Grothendieck (with M. Artin and J. L. Verdier), *Théorie des Topos et Cohomologie Etale des Schemas*(1963-64), Lecture Notes in Math. 269, 270, 305, Springer-Verlag, Berlin.

[7] A. Grothendieck, *Formule de Lefschetz et Rationalité des Fonctions L*, Séminaire Bourbaki, 1964/65, Exposé 279, W. A. Benjamin, New York , 1966.

[8] A. Grothendieck(by P. Deligne with J. F. Boutot, L. Illusie and J. L. Verdier), *Cohomologie Etale*, Lecture Notes in Mathematics, 569, Springer-Verlag, Berlin , 1977.

[9] A. Grothendieck, *Cohomologie l-adique et fonctions L*(1965-66), Lecture Notes in Math., 589, Springer-Verlag, Berlin, 1977.

[10] R. Hartshorne, *Algebraic Geometry*, GTM 52, Springer-Verlag, New York , 1977.

[11] H. Hasse, *Beweis des Analogons der Riemannschen Vermutung für die Artinschen und F. K. Schmidtshen Kongruenzzetafunktionen in gewissen elliptischen Fallen*, Ges. d. Wiss. Nachrichten. Math. Phys. Klasse. 1933, Heft 3, 253~262.

[12] L. K. Hua and H. S. Vandiver , *Characters over certain types of rings with applications to the theory of equations in a finite field*, Proc. Nat. Acad. Sci. U. S. A., **35**(1949), 94~99.

[13] N. Katz, *An overview of Deligne's proof of the Riemann hypothesis for varieties over finite fields*, Proc. Sympos. in Pure Math. Amer.

Math. Soc., **28**(1976), 275~305.

[14] A. Weil, *Numbers of solutions of equations in finite fields*, Bulletin of Amer. Math. Soc., **55**(1949), 497~508.

[15] A. Weil, *Sur les Courbes Algebriques et les Varietes qui s'en Deduisent*, Hermann, Paris , 1948.

第三章　局部域和整体域

§1　赋值和局部域

在这一节中，如无特殊说明，k 总表示一个有 q 个元素的有限域，$k(T)$ 是以 k 为常数域的有理函数域.

首先我们介绍有关赋值的一些基本概念和结果.

设 F 是一个域，F 上的一个**赋值**是一个从 F 到非负实数集的映射 v, 对 F 中任意元素 a 和 b, 它满足下述条件:

(a) $v(a)=0$ 的充要条件是 $a=0$;

(b) $v(ab)=v(a)v(b)$;

(c) 存在常数 C, 使得

$$v(a+b)\leq C\max\{v(a),v(b)\}.$$

例　(1) 对实数域 $\mathbf{R}$ 或复数域 $\mathbf{C}$, 通常其绝对值构成它上的一个赋值.

(2) 取 $v(0)=0$, 对域 F 上任意非零元 a, 取 $v(a)=1$, 这样定义了域 F 上的一个赋值，我们称之为 F 的 **平凡赋值**.

习题 1　证明上述条件 (c) 等价于：存在常数 C, 使得对任意满足 $v(a)\leq 1$ 的元素 a, 有

$$v(1+a)\leq C.$$

习题 2　设 v 为域 F 上的一个赋值，证明：若 u 为 F 中的单位根，则 $v(u)=1$. 特别地，有限域只有平凡赋值.

设 v 是域 F 的一个赋值，对 F 中任意元素 a, 我们定义 a 的基本邻域系如下:

$$U(a,\varepsilon)=\{b\in F\ :\ v(a-b)<\varepsilon\},$$

其中 ε 取遍正实数. 由此就在 F 上定义了一个拓扑 T_v.

习题 3 证明 T_v 是一个 Hausdorff 拓扑.

习题 4 若 v 是平凡赋值, 证明 T_v 是一个离散拓扑.

对域 F 上的两个赋值 v_1 和 v_2 , 如果它们定义了 F 上相同的拓扑结构, 我们称它们是 **等价** 的.

习题 5 设 v_1, v_2 是域 F 的两个非平凡赋值, 证明下面条件等价:

(1) 存在正实常数 α, 使得 $v_1 = v_2^{\alpha}$;

(2) $T_{v_1} = T_{v_2}$, 即 v_1 与 v_2 等价;

(3) T_{v_1} 是 T_{v_2} 的强拓扑;

(4) 若 $v_1(a) < 1$, 则一定有 $v_2(a) < 1$;

(5) 若 $v_1(a) \leq 1$, 则一定有 $v_2(a) \leq 1$.

对于域 F 上的赋值 v, 如果条件 (c) 中的常数可取为 1, 则称 v 是 **非 Archimedes 赋值**, 否则称为 **Archimedes 赋值**. 从上面习题可以看出, 等价的赋值或者同是非 Archimedes 的, 或者同是 Archimedes 的.

习题 6 设 v 是域 F 的一个赋值, 证明

(1) v 是非 Archimedes 的充要条件是集合 $\{v(n) : n \in Z\}$ 是有界的

(2) v 是 Archimedes 的充要条件是: 对 F 中任意两个元素 $a, b\ (a \neq 0)$, 总存在正整数 n, 使得 $v(na) \geq v(b)$.

显然, 平凡赋值是非 Archimedes 的, 而 **R** 或 **C** 上的绝对值则是 Archimedes 的.

习题 7 将赋值条件中的 (c) 改为

(d) **三角不等式** $\quad v(a+b) \leq v(a) + v(b)$.

证明: (1) 满足条件 (a), (b) 和 (d) 的映射 v 也是一个赋值.

(2) 对任何一个赋值, 均存在一个满足 (a), (b) 和 (d) 的赋值与之等价.

今后, 一提到赋值, 除非有特别的说明, 我们总假定它满足三角不等式.

赋值论由于它在数论、交换代数、代数几何中的应用而受到人

们的重视，在本书中，我们将仅限于讨论与数论相关的内容，对一般的赋值理论，有兴趣的读者可以参阅 Zariski, Samuel 的经典著作 [12] 或参考文献 [4], [9] 等有关文献.

接下来，我们将对具体的域 F 来加以讨论.

取 $F=k(T)$. 设 x 是 k 上射影直线 $\mathbf{P}^1$ 的一个闭点 (按 Zariski 拓扑). 要想了解 $\mathbf{P}^1$ 上一个非零有理函数 f 在 x 点处的性质，我们首先需要知道 f 在 x 点处是零点还是极点，或更精确一些，要知道 f 在 x 点处的阶 $v_x(f)$. 当 $v_x(f)>0$ 时，x 为 f 的 $v_x(f)=\mathrm{ord}_x f$ 阶零点，而当 $v_x(f)<0$ 时，它为 f 的 $-v_x(f)$ 阶极点. 求阶 $v_x(f)$ 的一个简单方法是利用 x 点的不可约多项式 $P(T)$, 首先将 $f(T)$ 写成多项式之商 $g(T)/h(T)$ (当 x 是 ∞ 点时，以 $1/T$ 代换 T), 则 f 在 x 点的阶正好等于多项式 $g(T)$ 的分解式中 $P(T)$ 的次数减去多项式 $h(T)$ 的分解式中 $P(T)$ 的次数. 用理想论的语言来说就是：设 $\mathfrak{P}$ 是 $k[T]$ 中由 $P(T)$ 生成的理想，则 $g(T)$ 中 $P(T)$ 的次数正好是集合 $\{m\in\mathbf{N}:g(T)\in\mathfrak{P}^m\}$ 中的最大整数 m. 这最后一种表述可以推广到 k 上的任意函数域 K 上去. 此时，K 的一个**位** (place) 是 $(k[T])$ 或 $k[1/T]$ 在 K 中整闭包 $\mathcal{O}$ 的极大理想. 为了解 $\mathcal{O}$ 中非零有理函数 f 在位 $\mathfrak{P}$ 处的性质，仍表 f 为 $\mathcal{O}$ 中两个多项式 g 和 h 的商 g/h, 由于 K 是 $\mathcal{O}$ 的商域，因此这种表示法总是可行的. 从而定义 $\mathcal{O}$ 中多项式 g 在位 $\mathfrak{P}$ 处的阶 $\mathrm{ord}_{\mathfrak{P}}g$ 是使 g 在理想 $\mathfrak{P}^m$ 中的最大整数 m, 从而定义 f 在 $\mathfrak{P}$ 处的**阶** $\mathrm{ord}_{\mathfrak{P}}f$ 为 $\mathrm{ord}_{\mathfrak{P}}g-\mathrm{ord}_{\mathfrak{P}}h$. 对 K 上的每个位 $\mathfrak{P}$, 我们可以定义 K 上的一个赋值为 $|\ |_{\mathfrak{P}}$ 为

$$\begin{cases}|0|_{\mathfrak{P}}=0,\\ |f|_{\mathfrak{P}}=N\mathfrak{P}^{-\mathrm{ord}_{\mathfrak{P}}f}=(q^{-\deg\mathfrak{P}})^{\mathrm{ord}_{\mathfrak{P}}f}=|\mathcal{O}/\mathfrak{P}|^{-\mathrm{ord}_{\mathfrak{P}}f},\end{cases}$$

其中 f 为 K 中任意非零元.

习题 8 证明如上定义的 $|\ |_{\mathfrak{P}}$ 确为域 K 上的一个赋值，并且是非 Archimedes 的.

在有理数域 $\mathbf{Q}$ 上，整数环 $\mathbf{Z}$ 扮演了有理函数域 $k(T)$ 中 $k[T]$

的角色. $\mathbf{Z}$ 中每个素理想 (p) 是 $\mathbf{Q}$ 的一个有限位. 若 K 是一个数域, 即 $\mathbf{Q}$ 的一个有限维 (代数) 扩张, 则 K 上整数环 $\mathcal{O}$ 是 $\mathbf{Z}$ 在 K 中的整闭包, 而 $\mathcal{O}$ 的极大理想 $\mathfrak{p}$ 则是 K 的有限位, 剩余类域 $\mathcal{O}/\mathfrak{p}$ 是一个有限域, 其势 $N\mathfrak{p}$ 称为理想 $\mathfrak{p}$ 的**范**. 同上面一样, 我们可以定义位 $\mathfrak{p}$ 处的阶 $\mathrm{ord}_{\mathfrak{p}}$, 进而可定义 K 上赋值 $|\ |_{\mathfrak{p}}$ 为

$$\begin{cases} |0|_{\mathfrak{p}} = 0, \\ |z|_{\mathfrak{p}} = N\mathfrak{p}^{\mathrm{ord}_{\mathfrak{p}} z} = |\mathcal{O}/\mathfrak{p}|^{-\mathrm{ord}_{\mathfrak{p}} z}, \quad z \in K^{\times}. \end{cases}$$

习题 9 设 K 是一个函数域数域, $\mathfrak{p}_1$ 和 $\mathfrak{p}_2$ 是 K 上两个不同的位, 它们分别定义了 K 上两个赋值 $|\ |_{\mathfrak{p}_1}$ 和 $|\ |_{\mathfrak{p}_2}$. 则这两个赋值是否等价? 为什么?

习题 10 设 K 是一个函数域或数域, $\mathfrak{p}$ 为 K 的一个位, 证明赋值 $|\ |_{\mathfrak{p}}$ 定义了 K 上的一个度量.

记 $K_{\mathfrak{p}}$ 为域 K 关于赋值 $\mathfrak{p}$ 所定义度量的完备化, 它是一个包含 K 的域, 并且 K 在 $K_{\mathfrak{p}}$ 中稠密. $K_{\mathfrak{p}}$ 中的整数是那些在位 $\mathfrak{p}$ 处没有极点的元 (即阶 $\mathrm{ord}_{\mathfrak{p}} x$ 非负的元 x), 它们的全体构成一个环, 称为 $K_{\mathfrak{p}}$ 的整数环, 记作 $\mathcal{O}_{\mathfrak{p}}$, 即

$$\mathcal{O}_{\mathfrak{p}} = \{x \in K_{\mathfrak{p}} : |x|_{\mathfrak{p}} \leq 1\}.$$

$\mathcal{O}_{\mathfrak{p}}$ 中乘法可逆元称为 **$\mathfrak{p}$-adic 单位**, 其全体构成了 $\mathcal{O}_{\mathfrak{p}}$ 的一个乘法子群 $\mathcal{U}_{\mathfrak{p}}$:

$$\mathcal{U}_{\mathfrak{p}} = \{x \in K_{\mathfrak{p}} : |x|_{\mathfrak{p}} = 1\}.$$

因此

$$\mathfrak{P}_{\mathfrak{p}} = \mathcal{O}_{\mathfrak{p}} - \mathcal{U}_{\mathfrak{p}} = \{x \in K_{\mathfrak{p}} : |x|_{\mathfrak{p}} < 1\}$$

是 $\mathcal{O}_{\mathfrak{p}}$ 的唯一极大理想, 且 $\mathcal{O}_{\mathfrak{p}}$ 的所有非零理想均为 $\mathfrak{P}_{\mathfrak{p}}$ 的幂, 商域 $\mathcal{O}_{\mathfrak{p}}/\mathfrak{P}_{\mathfrak{p}}$ 称为 $K_{\mathfrak{p}}$ 的**剩余类域**, 它与完备化前的剩余类域 $\mathcal{O}/\mathfrak{p}$ 是同构的, 从而也是有限的. 理想 $\mathfrak{P}_{\mathfrak{p}}$ 是一个主理想, 其生成元具有最大赋值 $(N\mathfrak{p})^{-1}$. 反过来, 具有赋值 $(N\mathfrak{p})^{-1}$ 的元一定生成 $\mathfrak{P}_{\mathfrak{p}}$. 我们以 $\varpi_{\mathfrak{p}}$ 表任意一个生成元, 称它是位 $\mathfrak{p}$ 的**局部单值化元**

素 (uniformizer). 于是, $K_{\mathfrak{p}}^{\times} = \mathcal{U}_{\mathfrak{p}} \times < \varpi_{\mathfrak{p}} \rangle$. 进一步, 设 S 为 $\mathcal{O}_{\mathfrak{p}}$ 中剩余类域的一个代表元集, 则 $\mathcal{O}_{\mathfrak{p}}$ 中任意元素均可写成系数在 S 中, 变数为 $\varpi_{\mathfrak{p}}$ 的 Taylor 级数. p-adic 单位是那些常数项不在 $\mathfrak{P}_{\mathfrak{p}}$ 中的元素, 而 $K_{\mathfrak{p}}$ 中的任意元素则可写成系数在 S 中, 变数为 $\varpi_{\mathfrak{p}}$ 的 Laurent 级数.

例　设 $K = \mathbf{Q}$, $\mathfrak{p} = (p)$, 则可取

$$\varpi_{\mathfrak{p}} = p, \quad S = \{i : 0 \le i \le p-1\}.$$

从而

$$\mathcal{O}_{\mathfrak{p}} = \mathbf{Z}_p = \left\{ \sum_{i=0}^{\infty} a_i p^i : 0 \le a_i \le p-1 \right\},$$

$$\mathbf{Q} \bigcap \mathbf{Z}_p = \left\{ \frac{m}{n} : m, n \in \mathbf{Z}, p \nmid n \right\},$$

$$\mathfrak{P}_{\mathfrak{p}} = p\mathrm{Z}_p = \left\{ \sum_{i=1}^{\infty} a_i p^i : 0 \le a_i \le p-1 \right\},$$

$$\mathcal{U}_{\mathfrak{p}} = \left\{ \sum_{i=0}^{\infty} a_i p^i : 0 \le a_i \le p-1,\ a_0 \ne 0 \right\},$$

$$\mathbf{Q}_p = \left\{ \sum_{i > -\infty} a_i p^i : 0 \le a_i \le p-1 \right\},$$

剩余类域 $\mathbf{Z}_p/p\mathbf{Z}_p \cong \mathbf{Z}/p\mathbf{Z}$.

例　设 $K = k(T)$, $\mathfrak{p}$ 是一个在 $a \in k$ 处的次数为 1 的位. 取 $\varpi_{\mathfrak{p}} = T - a$, $S = k$, $\mathcal{O}_{\mathfrak{p}}$ 是由系数在 k 中 $T-a$ 的 Taylor 级数构成的, $\mathcal{U}_{\mathfrak{p}}$ 则由那些在 a 处不为 0 的 Taylor 级数构成. 在 $\mathfrak{p}$ 处的剩余类域同构于 k. 域 $K_{\mathfrak{p}}$ 是形式幂级数域 $k((T-a))$, 它同构于形式幂级数域 $k((T))$.

习题 11　(1) 将 $\mathbf{Q}$ 中元素 -1 和 $1/r$, 其中 $p \nmid r$, 展成系数在 S 中, 变数为 p 的 Taylor 级数.

(2) 将 $k(T)$ 中元素 $1/(T-b)$ $(b \ne a)$ 展成系数在 k 中, 变数为 $T-a$ 的 Taylor 级数.

由于赋值 $|\ |_{\mathfrak{p}}$ 定义了 K 上的度量，故给出了 $K_{\mathfrak{p}}$ 上的一个拓扑，容易验证，$K_{\mathfrak{p}}$ 关于这个拓扑是一个拓扑域 (即域运算关于此拓扑是连续的). 理想集 $\{\mathfrak{P}_{\mathfrak{p}}^n : n \geq 0\}$ 构成 0 的邻域系，使得 $K_{\mathfrak{p}}$ 作为一个加法拓扑群是局部紧的，且为全不连通的 (即每个点都是一个连通分支，或既开又闭的). 从而 $\mathcal{O}_{\mathfrak{p}}$ 以及 $\mathfrak{P}_{\mathfrak{p}}^n$ $(n \geq 1)$ 也是既开又闭的. 单位群 $\mathcal{U}_{\mathfrak{p}}$ 有一个自然的滤链 (filtration)

$$\mathcal{U}_{\mathfrak{p}} \supset 1 + \mathfrak{P}_{\mathfrak{p}} \supset 1 + \mathfrak{P}_{\mathfrak{p}}^2 \supset \cdots$$

(关于滤链可参阅参考文献 [2], 不过对于初学者而言，只须承认它即可), 并且有下面关系：

$$\mathcal{U}_{\mathfrak{p}}/1 + \mathfrak{P}_{\mathfrak{p}} \cong (\mathcal{O}_{\mathfrak{p}}/\mathfrak{P}_{\mathfrak{p}})^{\times},$$

$$1 + \mathfrak{P}_{\mathfrak{p}}^k/1 + \mathfrak{P}_{\mathfrak{p}}^{k+1} \cong \mathcal{O}_{\mathfrak{p}}/\mathfrak{P}_{\mathfrak{p}}, \quad k = 1, 2, \cdots.$$

从而群集 $\{1 + \mathfrak{P}_{\mathfrak{p}}^n : n \geq 1\}$ 构成了 1 的一个邻域系，使得乘法群 $K_{\mathfrak{p}}^{\times}$ 也是局部紧的，而且 $\mathcal{U}_{\mathfrak{p}}$ 是既开又紧的. 注意这里 $K_{\mathfrak{p}}^{\times}$ 上的拓扑是由 $K_{\mathfrak{p}}$ 的拓扑诱导出而得的.

上面讨论的赋值是非 Archimedes 赋值，于是位 $\mathfrak{p}$ 被称为 K 的**非 Archimedes 位**或**有限位**. 当 K 是一个函数域时，K 的所有赋值都是非 Archimedes 的. 但当 K 为数域时，Archimedes 赋值是存在的，它们导出 K 的 Archimedes 位或无限位. 更精确一些，设 K 为 $\mathbf{Q}$ 上的 n 次数域，则存在 $\xi \in K$, 使得 $K = \mathbf{Q}(\xi)$, ξ 在 $\mathbf{Q}$ 上的不可约多项式 $f(x)$ 次数为 n. 设 $\xi_1, \cdots, \xi_r$ 多项式 $f(x)$ 的实根，$\xi_{r_1+1}, \overline{\xi}_{r_1+1}, \cdots, \xi_{r_1+r_2}, \overline{\xi}_{r_1+r_2}$ 为其复根，则 $n = r_1 + 2r_2$. 这里 $\overline{\xi}$ 表复数 ξ 的共轭. 域 K 到 $\mathbf{C}$ 中的 n 个 $\mathbf{Q}$ 嵌入定义为

$$\sigma_i : \xi \longmapsto \xi_i, \quad i = 1, \cdots, r_1$$

和

$$\tau_j : \xi \longmapsto \xi_{r_1+j}, \quad j = 1, \cdots, r_2.$$

于是 $\sigma_i(K)$ 为 $\mathbf{R}$ 的子域，$\tau_j(K)$ 为 $\mathbf{C}$ 的子域，由通常 $\mathbf{R}$ 或 $\mathbf{C}$ 的绝对值在嵌入像上的限制就可诱导出 K 上的赋值，而且 K 关于

这些赋值的完备化就是 $\mathbf{R}$ 或 $\mathbf{C}$. 另一方面，注意到嵌入 τ_j 与 $\overline{\tau_j}$ 诱导出 K 上同一个赋值，而 $\sigma_1, \cdots, \sigma_{r_1}, \tau_1, \cdots, \tau_{r_2}$ 则给出 K 上不等价的赋值，它们统称为 K 上的 **Archimedes 赋值**. 我们说 K 有 r_1 个实位和 r_2 个复位.

习题 12　(1) 验证这 $r_1 + r_2$ 个赋值是 Archimedes 的赋值.

(2) 证明由 $\sigma_1, \cdots, \sigma_{r_1}, \tau_1, \cdots, \tau_{r_2}$ 诱导出的这 $r_1 + r_2$ 个赋值两两互不等价.

一个域如果是数域或者是常数域为有限域的单变量函数域，则称之为**整体域**. 设 v 是整体域 K 的一个位，则 K 在 v 处的完备化 K_v 称为是**局部域**. 于是局部只能是 $K_\mathfrak{p}$, $\mathbf{R}$ 或 $\mathbf{C}$. 我们也称 $\mathbf{R}$ 和 C 为 **Archimedes 局部域**, $K_\mathfrak{p}$ 为非 **Archimedes 局部域**. 注意，局部域都是局部紧的. K_v 上的**标准赋值** $|\ |_v$ 定义为:

$$|\ |_v = \begin{cases} |\ |_\mathfrak{p}, & 若 K_v = K_\mathfrak{p}, \\ |\ |_\mathbf{R}, & 若 K_v = \mathbf{R}, \\ |\ |_\mathbf{C}^2, & 若 K_v = \mathbf{C}. \end{cases}$$

在复数 $\mathbf{C}$ 的情形，标准赋值的取法是由于两个共轭的复嵌入导出同一个复位这一个事实而得的.

整体域上的每个非 Archimedes 位对应了一个赋值的等价类，其中如上定义的称为**标准赋值**, 这样选择的原因是为了便于后面讨论乘积公式. 赋值论中一个著名结果是：一个整体域的任意非平凡赋值等价于 $|\ |_\mathbf{R}$ 或 $|\ |_\mathbf{C}$ 或某个标准的 $\mathfrak{p}$-adic 赋值(参见参考文献 [12] 或 [4], [9] 等).

下面我们以一个十分重要且又基本的结论——Hensel 引理来结束这一节.

Hensel 引理　令 K 是一个非 Archimedes 局部域，其整数环为 $\mathcal{O}$, 极大理想为 $\mathfrak{p}$. 又设 $F(x)$ 为系数在 $\mathcal{O}$ 中的一个多项式. 假设 $F(x)$ 模 $\mathfrak{p}$ 后所得的函数 $\overline{F}(x)$ 可写成系数在 $\mathcal{O}/\mathfrak{p}$ 中的互素多项式 $g(x)$ 和 $h(x)$ 的乘积，则存在系数在 $\mathcal{O}$ 中的多项式 $G(x)$ 和

$H(x)$, 它们模 $\mathfrak{p}$ 后分别等于 $g(x)$ 和 $h(x)$, 使得

$$F(x)=G(x)H(x),\ \text{且}\ \deg G=\deg g.$$

证 设 $G_0(x)$ 和 $H_0(x)$ 分别为 $g(x)$ 和 $h(x)$ 在 $\mathcal{O}[x]$ 中的一个提升. 换句话说, $\mathcal{O}$ 上多项式 $G_0(x)$ 和 $H_0(x)$ 模 $\mathfrak{p}$ 后分别为 $g(x)$ 和 $h(x)$, 并且 $\deg G_0=\deg g$, $\deg H_0=\deg h$. 则

$$F(x)-G_0(x)H_0(x)=\varpi F_1(x),$$

这里 ϖ 是 $\mathfrak{p}$ 的局部单值化元素, $F_1(x)\in\mathcal{O}[x]$, $\deg F_1\le\deg F$. 下一步解方程

$$F(x)\equiv(G_0(x)+\varpi g_1(x))(H_0(x)+\varpi h_1(x))\ (\bmod\ \mathfrak{p}^2),$$

其中 $g_1,h_1\in\mathcal{O}[x]$. 这等于说求解方程

$$F_1(x)\equiv g_1(x)H_0(x)+h_1(x)G_0(x)\ (\bmod\ \mathfrak{p}).$$

或等价地, 在 $\mathcal{O}/\mathfrak{p}[x]$ 中求解方程

$$\overline{F_1(x)}=\overline{g_1(x)}h(x)+\overline{h_1(x)}g(x).$$

由于 g,h 是互素的, 故后一个方程是可解的. 我们选择 $\overline{g_1}$ 和 $\overline{h_1}$, 使得 $\deg\overline{g_1}<\deg g$ (那么自然地有 $\deg\overline{h_1}\le\deg F-\deg g$). 又设 g_1,h_1 分别为 $\overline{g_1}$ 和 $\overline{h_1}$ 在 $\mathcal{O}[x]$ 中的提升, 使得

$$\deg g_1=\deg\overline{g}_1\quad\text{和}\quad\deg h_1=\deg\overline{h}_1.$$

则取

$$G_1(x)=G_0(x)+\varpi g_1(x)\quad\text{和}\quad H_1(x)=H_0(x)+\varpi h_1(x),$$

从而有 $\deg G_1=\deg g$, $\deg H_1\le\deg F-\deg g$, $\overline{G_1}=g$, $\overline{H_1}=h$, 并且存在 $F_2\in\mathcal{O}[x]$, 使得

$$F-G_1H_1=\varpi^2F_2,$$

显然, $\deg F_2\le\deg F_1\le\deg F$. 同上面一样继续求解方程

$$F(x)\equiv(G_1(x)+\varpi^2g_2(x))(H_1(x)+\varpi^2h_2(x))\ \ (\bmod\ \mathfrak{p}^3),$$

且将此过程进行下去，我们将得到两个多项式序列 $\{G_0, G_1, \cdots\}$ 和 $\{H_0, H_1, \cdots\}$，其中

$$\deg G_{i+1} = \deg G_i\,,\quad G_{i+1} \equiv G_i \pmod{\mathfrak{p}^{i+1}}\,,$$
$$H_{i+1} \equiv H_i \pmod{\mathfrak{p}^{i+1}}\,,\quad F(x) \equiv G_i(x)H_i(x) \pmod{\mathfrak{p}^{i+1}}\,.$$

从而这是两个 Cauchy 序列．取极限，设它们分别收敛于 $G(x)$ 和 $H(x)$，则显然有，$\deg G = \deg G_0 = \deg g$，$\overline{G} = g$，$\overline{H} = h$，及 $F(x) = G(x)H(x)$，由此引理得证．

习题 13 设 $\mathfrak{p}$ 为整体域 K 上的有限位，多项式

$$f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$$

的系数 $a_{n-1}, \cdots, a_0$ 都在 $\mathfrak{p}$ 中，但 a_0 不在 $\mathfrak{p}^2$ 中，证明 $f(x)$ 不可约 (这是 Eisenstein 不可约判别法的推广)．进而讨论多项式 x^2+1，x^2+2 及 x^2+3 在 3-adic 数域 $\mathbf{Q}_3$ 中的因式分解．

习题 14 设 K 是常数域为 k 的单变量函数域，v 为 K 上次数为 n 的有限位，设 ϖ_v 为 K_v 的任意局部单值化元素，证明 K 同构于形式幂级数域 $k_n((\varpi_v))$．

§2 赋值的扩张

设 K 是一个关于赋值 $|\ |_K$ 的非 Archimedes 局部域，L 是 K 的 n 次可分扩张，$\overline{K}$ 为 K 的代数闭包，那么存在 n 个 K 上的由 L 到 $\overline{K}$ 中的嵌入 $\sigma_1, \cdots, \sigma_n$．关于这 n 个嵌入我们可以定义 L 中元素 z 的**迹**

$$\mathrm{Tr}_{L/K}(z) = \sigma_1(z) + \cdots + \sigma_n(z)$$

与**范**

$$\mathrm{N}_{L/K}(z) = \sigma_1(z) \cdots \sigma_n(z).$$

可以证明，迹映射是从加法群 L 到加法群 K 的一个同态；范映射则是乘法群 $L^\times$ 到乘法群 $K^\times$ 的一个同态．进一步，若 M 是

L 的一个包含 K 的子域，则

$$\mathrm{Tr}_{L/K}=\mathrm{Tr}_{M/K}\circ\mathrm{Tr}_{L/M},$$

$$\mathrm{N}_{L/K}=\mathrm{N}_{M/K}\circ\mathrm{N}_{L/M}.$$

有关元素 z 的迹 $\mathrm{Tr}_{L/K}(z)$ 和范 $\mathrm{N}_{L/K}(z)$ 同它在 K 上的不可约多项式的系数之间的关系是与有限域时的情形一样的(参见第一章)。这些关系的阐述及上述结论的证明，我们作为练习留给读者完成.

在这一节中，我们感兴趣的是如何将 K 上的赋值 $|\ |_K$ 扩张为 L 的赋值 $|\ |_L$. 假定这样是可以做到的，当 L 为 K 的 Galois 扩张时，z 的所有共轭有同样的赋值，因此

$$|z|_L^n=|\sigma_1(z)|_L\cdots|\sigma_n(z)|_L=|\mathbf{N}_{L/K}(z)|_L=|\mathbf{N}_{L/K}(z)|_K.$$

这表明

$$|z|_L=|\mathbf{N}_{L/K}(z)|_K^{1/n}.$$

注意这个公式在 L 不是 K 的 Galois 扩张时也是有意义的. 下面的定理是说这个公式的确给出赋值 $|\ |_K$ 在 L 上的扩张.

定理 1 设 K 为具有非 Archimedes 赋值 $|\ |_K$ 的局部域，L 是 K 的次数为 n 的域扩张，则 $|\ |_K$ 在 L 上有唯一的一个的赋值扩张 $|\ |_L$，它由下式给出

$$|z|_L=|\mathbf{N}_{L/K}(z)|_K^{1/n},\quad z\in L.$$

更进一步，域 L 关于该赋值还是完备的.

证 先证存在性. 对 L 中元素 z，定义

$$|z|_L=|\mathbf{N}_{L/K}(z)|_K^{1/n}.$$

显然，要证 $|\ |_L$ 就是我们所需要的赋值，只需证明：对 L 中任意元素 z 和 w，均有三角不等式 $|z+w|_L\le\max(|z|_L,|w|_L)$ 成立. 这等价于证明对 L 中满足 $|\mathbf{N}_{L/K}(z)|_K\le 1$ 的任意元素 z，均有

$$|\mathbf{N}_{L/K}(1+z)|_K\le 1.$$

设 $f(x)=x^m+a_{m-1}x^{m-1}+\cdots+a_0$ 是 z 在 K 上的不可约多项式. 由根与系数的关系

$$(a_0(-1)^m)^{n/m}=\mathbf{N}_{L/K}(z)$$

可得 $|a_0|_K\leq 1$. 换句话说, a_0 是 K 上的整数, 即 $a_0\in\mathcal{O}_K$. 又因

$$\begin{aligned}f(-1)&=(-1)^m\mathbf{N}_{K(z)/K}(1+z)\\&=(-1)^m+(-1)^{m-1}a_{m-1}+\cdots+a_0.\end{aligned}$$

所以如果我们能证明所有系数 a_i 均是 K 上的整数的话, 那么由赋值定义即得 $\mathbf{N}_{K(z)/K}(1+z)$ 也是 K 的整数. 进而 $\mathbf{N}_{L/K}(1+z)$ 为 K 上的整数, 故它在 K 上赋值 $|\mathbf{N}_{L/K}(1+z)|\leq 1$, 从而存在性得证.

现在我们就来证所有的系数 a_i 均为 K 上的整数. 如若不然. 设 j 是使 $|a_j|_K\geq|a_i|_K$ $(i=0,\cdots,m-1)$ 的最大下标. 则由假设知 $|a_j|_K>1$ 且 $j>0$, 而当 $i>j$ 时, $|a_i|_K<|a_j|_K$. 以 $\mathfrak{p}_K$ 表示 $\mathcal{O}_K$ 的最大理想, 则有 $a_j^{-1}\in\mathfrak{p}_K$, 以及对任意的满足 $m-1\geq i>j$ 的 i, 有 $a_ia_j^{-1}\in\mathfrak{p}_K$. $\mathcal{O}_K[x]$ 中的多项式 $a_j^{-1}f(x)$ 的系数皆 mod $\mathfrak{p}_K$ 后得

$$\overline{a_j^{-1}f(x)}=g(x)h(x),$$

其中 $h(x)=1$, $g(x)=\overline{a_j^{-1}f(x)}=x^j+\cdots$ 为一个 $\mathcal{O}_K/\mathfrak{p}_K[x]$ 中的 j 次多项式 (注意 $0<j<m$). 利用 Hensel 引理得, 存在 $\mathcal{O}_K[x]$ 中两个多项式 G 与 H, 其中 G 的次数为 $j<m$, 使得

$$a_j^{-1}f(x)=G(x)H(x),$$

从而多项式 H 的次数为 $m-j>0$. 但这与 f 的不可约性矛盾, 由此证明了所有系数 a_j 均应为 K 上的整数.

现证唯一性. 将 L 视作 K 上的 n 维向量空间, $|\ |_K$ 在 L 上的扩充赋值 $\|\ \|$ 应满足

$$\|\alpha x\|=|\alpha|_K\,\|x\|,\quad \alpha\in K,\ x\in L.$$

给定 L 在 K 上的一组基 $\{\omega_1,\cdots,\omega_n\}$, 对 L 中任意元素 x, 记

$$x = \alpha_1\omega_1 + \cdots + \alpha_n\omega_n, \quad \alpha_i \in K.$$

定义 $\|x\|_0 = \max\limits_i |\alpha_i|_k$, 显然，它是 L 上的一个范数. 若 $\|\ \|$ 作为 L 上的范数等价于 $\|\ \|_0$, 则 L 上任何 $|\ |_K$ 的扩充赋值均互相等价，从而得到 $|\ |_L$ 的唯一性. 又因为 L 关于 $\|\ \|_0$ 是完备的，所以完备性也由此得到. 于是定理 1 可由下述结果得证.

定理 2 设 K 是一个具有赋值 $|\ |_K$ 的局部域，L 为 K 上有限维向空间，则 L 上任意满足关系

$$\|\alpha x\| = |\alpha|_K \|x\|, \quad \alpha \in K,\ x \in L$$

的范数 $\|\ \|$ 均等价于前面所定义的范数 $\|\ \|_0$. 此外，L 关于该范数是完备的.

证 我们只需证，存在正常数 μ 和 ν, 使得对任意的 $x \in L$，有

$$\|x\| \le \mu\|x\|_0 \quad \text{和} \quad \|x\|_0 \le \nu\|x\|.$$

现取 $\mu = \|\omega_n\| + \cdots + \|\omega_n\|$, 对 $x = \alpha_1 w_1 + \cdots + \alpha_n\omega_n \in L$, 我们有

$$\begin{aligned}\|x\| &= \|\alpha_1\omega_1 + \cdots + \alpha_n\omega_n\| \\ &\le \|\alpha_1\omega_1\| + \cdots + \|\alpha_n\omega_n\| \\ &= |\alpha_1|_K \|\omega_1\| + \cdots + |\alpha_n|_K \|\omega_n\| \le \mu\|x\|.\end{aligned}$$

从而第一个不等式得证.

为证第二个不等式，仍记 $x = \alpha_1\omega_1 + \cdots + \alpha_n\omega_n$. 定义 $|x|_i = |\alpha_i|_K$. 显然，我们只需要证明存在正常数 $\nu_1,\cdots,\nu_n$, 使得 $|x|_i \le \nu_i\|x\|$. 当 $n=1$ 时这是明显的；归纳假设 $n-1$ 时断言为真，在 n 时，设 V 是由 $\omega_1,\cdots,\omega_{n-1}$ 在 K 上张成的 $n-1$ 维子空间，记 $\|\ \|'$ 为 $\|\ \|$ 在 V 上的限制. 由归纳假设，我们在 V 上总可找到 $\nu_1',\cdots,\nu_{n-1}'$, 使得 $\|\ \|'$ 等价于 $\|\ \|_0'$, 且 V 是完备的. 若 ν_n 也存

在，记 $x = x(V) + \alpha_n\omega_n$，这里 $x(V) = \alpha_1\omega_1 + \cdots + \alpha_{n-1}\omega_{n-1}$ 为 x 在 V 上的投影. 则当 $1 \le i \le n-1$ 时，

$$|x|_i = |x(V)|_i \le \nu_i' \|x(V)\|' \le \nu_i'(\|x\| + \|\alpha_n\omega_n\|)$$
$$\le \nu_i'(\|x\| + |x|_n\|\omega_n\|) \le \nu_i'(1 + v_n\|\omega\|)\|x\|.$$

于是我们可取 $\nu_i = \nu_i'(1 + v_n\|\omega_n\|)$，进而此时 $\nu_1, \cdots, \nu_{n-1}$ 也是存在的，故定理正确. 若 ν_n 不存在，则存在 L 中序列 $\{x_j\}_{j\ge1}$，使得 $|x_j|_n > n\|x_j\|$. 显然 $x_j \notin V$. 又因该不等式在乘上非零常数后保持不变，故可设

$$x_j = \alpha_{j1}\omega_1 + \cdots + \alpha_{jn-1}\omega_{n-1} + \omega_n, \quad \alpha_{ji} \in K.$$

这表明 $\|x_j\| < 1/j$. 因此当 $j \to \infty$ 时，$x_j \to 0$. 于是

$$\lim_{j\to\infty}(x_j - \omega_n) = -\omega_n;$$

另一方面，$x_j - \omega_n$ 为闭子空间 V 中元素，不可能在 V 外有极限点，这就导出矛盾，从而 ν_n 一定存在，故 $\nu_1, \cdots, \nu_{n-1}$ 也一定存在. 利用归纳法，定理断言成立.

注 (1) 以 $\mathcal{O}_L$ 表示域 L 关于赋值 $|\ |_L$ 的整数环，可以证明 $\mathcal{O}_L$ 中的任意元素在 $\mathcal{O}_K$ 上是整的；反过来，对 L 中元素 x，若它在 $\mathcal{O}_K$ 上是整的，则其范数应在 $\mathcal{O}_K$ 中，因此它也应在 $\mathcal{O}_L$ 中. 从而 $\mathcal{O}_L$ 是由那些在 K 上整的 L 中的元素构成的. 换句话说，两个"整"的概念是一致的.

(2) 定理 1 对 Archimedes 局部域也是成立的. 这是因为 $|z|_{\mathbf{C}} = |z\bar{z}|_{\mathbf{R}}^{1/2}$ $(z \in \mathbf{C})$ 也是 $\mathbf{C}$ 上的一个赋值，而唯一性的证明对域 $\mathbf{C}$ 也是成立的.

习题 15　完成上面注中断言的证明.

习题 16　在上面注 (1) 的假设下，证明

$$\mathrm{Tr}_{L/K}(\mathcal{O}_L) \supseteq \mathcal{O}_K.$$

在定理 1 的记号与假设下，我们用 $\mathcal{O}_L, \mathcal{O}_K$ 分别表示 L, K 中的整数环，用 $\mathfrak{p}_L$ 和 $\mathfrak{p}_K$ 分别表示 $\mathcal{O}_L$ 和 $\mathcal{O}_K$ 中的极大理想，且

$\mathcal{O}_K \bigcap \mathfrak{p}_L = \mathfrak{p}_K$. 剩余类域 $\mathcal{O}_L/\mathfrak{p}_L$ 为剩余类域 $\mathcal{O}_K/\mathfrak{p}_K$ 的扩张. 设 $\omega_1, \cdots, \omega_f$ 为 $\mathcal{O}_L$ 中一组元素，它们模 $\mathfrak{p}_L$ 后所得的元 $\overline{\omega}_1, \cdots, \overline{\omega}_f$ 是 $\mathcal{O}_K/\mathfrak{p}_K$ 线性无关的，那么我们可以断言 $\omega_1, \cdots, \omega_f$ 在 K 上也是线性无关的. 事实上，如果它们有一个非平凡的线性关系

$$a_1\omega_1 + \cdots + a_f\omega_f = 0,$$

可以假定 $a_i \in \mathcal{O}_K$, 并且不是所有的 a_i 都在 $\mathfrak{p}_K$ 中. 模 $\mathfrak{p}_L$ 后，上式给出了一个关于 $\overline{\omega}_1, \cdots, \overline{\omega}_f$ 的非平凡线性关系，这与 $\overline{\omega}_1, \cdots, \overline{\omega}_f$ 的线性无关性矛盾. 上面这一断言就说明了 $\mathcal{O}_L/\mathfrak{p}_L$ 为 $\mathcal{O}_K/\mathfrak{p}_K$ 的一个次数 $f \leq n = [L:K]$ 的有限扩张，常数 f 称为扩张 L/K 的**剩余类域次数**. 我们固定 K 中局部单值化元素 ϖ_K 和 L 中局部单值化元素 ϖ_L, 由于 $\varpi_K \in \mathfrak{p}_L$, 所以存在正整数 e, 使得 $\varpi_K = u\varpi_L^e$, 其中 u 为 L 中的单位. 从而

$$|\varpi_K|_L = |\varpi_L|_L^e,$$

我们称 e 为扩张 L/K 的**分歧指数**.

定理 3 设 K, L, e, f 如上定义，则

$$[L:K] = n = ef.$$

证 设 S 为剩余类域 $\mathcal{O}_L/\mathfrak{p}_L$ 在 $\mathcal{O}_L$ 中的一个代表元集. 我们知道，L 中任意非零元均都可以写成一个系数在 S 中，变数为 ϖ_L 的幂级数. 此外，对任意整数 j, 由于 ϖ_L^j 总可以写成 $u_j\varpi_L^i\varpi_K^m$ 的形式，其中 $u_j \in \mathcal{U}_L$, i 和 m 为整数且 $0 \leq i \leq e-1$. 于是 L 中的每个元素均可写成

$$\sum_{i=0}^{e-1} \sum_{m>-\infty} s_{im}\varpi_L^i\varpi_K^m$$

形式，其中 $s_{im} \in S$. 设 S 是剩余类域 $\mathcal{O}_K/\mathfrak{p}_K$ 在 $\mathcal{O}_K$ 中的一个代表元集，又设 $\omega_1, \cdots, \omega_f$ 为 $\mathcal{O}_L$ 中一组元素，使得模 $\mathfrak{p}_L$ 后，它们构成 $\mathcal{O}_L/\mathfrak{p}_L$ 在 $\mathcal{O}_K/\mathfrak{p}_K$ 上的一组基. 则我们可选择 S 为集合

$\{s_j\omega_j : s_j \in S, 1 \leq j \leq f\}$. 这表明 $\omega_j \varpi_L^i$ $(1 \leq j \leq f, 0 \leq i \leq e-1)$ 在 K 上生成了作为线性空间的域 L.

现在还需要证明 $\omega_j \varpi_L^i (1 \leq j \leq f, 0 \leq i \leq e-1)$ 在 K 上是线性无关的. 如若不然, 设

$$\sum_{i,j} a_{ij}\omega_j \varpi_L^i = 0$$

是 K 上一个非平凡的线性关系, 其中 i 与 j 的求和范围是 $1 \leq j \leq f$ 和 $0 \leq i \leq e-1$. 我们可假设所有的 a_{ij} 均在 $\mathcal{O}_K$ 中, 且存在一些 a_{ij} 是单位. 设

$$i_0 = \min\{m : 存在\ j,\ 使得\ a_{mj}\ 为单位\}.$$

那么当 $i < i_0$ 时, 对任意的 j, $a_{ij} \in \mathfrak{p}_K$. 从而

$$\sum_{\substack{i,j \\ i \neq i_0}} a_{ij}\omega_j \varpi_L^i \in \mathfrak{p}_L^{i_0+1}.$$

于是 $\sum_{1 \leq j \leq f} a_{i_0 j}\omega_j \varpi_L^{i_0} \in \mathfrak{p}_L^{i_0+1}$, 即 $\sum_{1 \leq i \leq f} a_{i_0 j}\omega_j \in \mathfrak{p}_L$. 模 $\mathfrak{p}_L$, 我们在 $\mathcal{O}_L/\mathfrak{p}_L$ 中就得到关系

$$\sum_{i=1}^{f} \overline{a_{i_0 j}}\ \overline{\omega_j} = 0.$$

这是 $\mathcal{O}_K/\mathfrak{p}_K$ 上一个非平凡的线性关系, 与 $\overline{\omega_1}, \cdots, \overline{\omega_f}$ 在 $\mathcal{O}_K/\mathfrak{p}_K$ 上的线性无关性矛盾. 从而假定错误, 这样我们就证明了 $\omega_1 \varpi_L^i$ $(1 \leq j \leq f, 0 \leq i \leq e-1)$ 构成 L 在 K 上的一组基, 定理得证.

以 q 表示剩余类域 $\mathcal{O}_K/\mathfrak{p}_K$ 的势. 假设 $|\ |_K$ 为 K 上使得 $|\varpi_K|_K = q^{-1}$ 的标准赋值, $|\ |_L$ 为 $|\ |_K$ 在 L 上唯一的扩张. 又以 $|\ |$ 表示 L 中等价于 $|\ |_L$ 的标准赋值. 于是

$$|\varpi_L| = |\mathcal{O}_L/\mathfrak{p}_L|^{-1} = q^{-f}.$$

我们希望能精确地描述赋值 $|\ |$. 为此, 利用定理 3 可得

$$|\varpi_K| = |\varpi_L|^e = q^{-ef} = q^{-n} = |\varpi_K|_K^n.$$

由此就知道$|\ |$在 K 上限制恰为$|\ |_K^n$. 结合定理 1, 我们即得到下面结论.

推论 1 设 K 为具有标准赋值$|\ |_K$ 的局部域, L 为 K 的 n 次可分扩张; 又设$|\ |_L$ 为$|\ |_K$ 在 L 上的扩张. 那么等价于$|\ |_L$ 的标准赋值可由下式给出

$$|x| = |\mathrm{N}_{L/K}x|_K, \quad x \in L.$$

习题 17 设 K 是一个非 Archimedes 局部域, L 为 K 上 n 次可分扩张. 设剩余类域 $\mathcal{O}_K/\mathfrak{p}_K$ 的势为 q, 剩余类域 $\mathcal{O}_L/\mathfrak{p}_L$ 的势为 q^f, 扩张的分歧指数是 e. 则 $n = ef$.

(1) 证明 L 中含有一个 $q^f - 1$ 次单位根 (提示: 利用 Hensel 引理).

(2) 设 ξ 为 L 中的 $q^f - 1$ 次单位根, $M = K(\xi)$. 证明 M 是 K 的一个次数为 f 的非分歧扩张, 即扩张 M/K 的分歧指数是 1; L 为 M 的全分歧扩张, 即扩张 M/K 的剩余类域次数为 1. 事实上, K 在 L 中的任意非分歧扩张均含于 M 中, 故也称 M 为 K 在 L 中的**极大不分歧扩张**.

(3) 设 ϖ_L 为 $\mathfrak{p}_L$ 中的局部单值化元素. 设 $f(x) = x^r + a_{r-1}x^{r-1} + \cdots + a_0$ 是 ϖ_L 在 M 中的不可约多项式, 证明: $a_i \in \mathfrak{p}_M, a_0 \in \mathfrak{p}_M - \mathfrak{p}_M^2$, 以及 $r = e$. 进而证明 $L = M(\varpi_L)$.

习题 18 设 K 是一个非 Archimedes 局部域, $M/K, L/M$ 均为有限可分代数扩张, 证明它们的分歧指数与剩余类域次数之间有下关系:

$$e_{L/K} = e_{L/M} \cdot e_{M/K}, \quad f_{L/K} = f_{L/M} \cdot f_{M/K}.$$

设 K 是一个域, L 为 K 的 n 次扩张, 记 $1 = \omega_1, \cdots, \omega_n$ 是 L 在 K 上的一组基, 则

$$\omega_i\omega_j = \sum_{k=1}^{n} a_{ijk}\,\omega_k, \quad a_{ijk} \in K. \tag{2.1}$$

注意: 在同构意义下, 这些关系唯一确定 L. 设 A 是一个包含 K 的环, 张量积 $A \bigotimes_K L$ 由 $\sum\limits_{i=1}^{n} c_i\omega_i$ 组成, 其中 $c_i \in A$. 从代数角度看, 这个张量积是一个环, 其中加法由分量加法给出, 乘法则由

(2.1) 式给出. 注意到 A 和 L 均可嵌入进 $A\bigotimes_K L$ 中去，所以如果在 A 上定义有拓扑的话，由 A^n 上的积拓扑，以及同构

$$(c_1,\cdots,c_n)\in A^n\longmapsto\sum_{i=1}^{n}c_i\omega_i\in A\bigotimes_K L$$

就可以诱导出 $A\bigotimes_K L$ 上的拓扑.

习题 19　证明张量积 $A\otimes_K L$ 上的代数结构及拓扑结构都不依赖于基 $\{\omega_1,\cdots,\omega_n\}$ 的选择.

定理 1 指出了一个局部域的赋值在该域的任意有限扩张上有唯一的扩张. 下面这个定理则要解释当基域是整体域时的情况.

定理 4　设 K 是一个整体域，L 为 K 的 n 次可分扩张. 又设 v 是 K 的一个位，则至多有 n 个 L 的位可整除 v, 即 K 上的赋值 $|\ |_v$ 至多可扩张为 n 个 (不等价的) L 的赋值. 设 $w_1,\cdots,w_r$ $(r\le n)$ 为 L 的所有能整除 v 的位，分别用 K_v 和 L_{w_i} 来表示 K 和 L 关于对应位的完备化. 则我们有下面代数和拓扑上的同构

$$K_v\bigotimes_K L\cong L_{w_1}\bigoplus\cdots\bigoplus L_{w_r},\tag{2.2}$$

其中等式右边赋以积拓扑.

证　由假设可知，存在元素 $\xi\in L$ 使得 $L=K(\xi)$. 设 $f(x)$ 为 ξ 在 K 上的不可约多项式，将 $f(x)$ 在 K_v 上分解为不可约因子的乘积 $f(x)=f_1(x)\cdots f_r(x)$. 由于扩张 L/K 是可分的，故 f_i 两两互素. 显然 $r\le n$, 于是利用中国剩余定理，在代数上有

$$\begin{aligned}K_v\bigotimes_K L&\cong K_v\bigotimes_K K[x]/(f(x))\cong K_v[x]/(f(x))\\&\cong\prod_{i=1}^{r}K_v[x]/(f_i(x)),\end{aligned}$$

这里每个 $K_v[x]/(f(x))$ 均为 K_v 的有限域扩张. 在上面同构中，元素 ξ 在 $K_v[x]/(f(x))$ 中被映为 $x+(f(x))$, 故它在 $\prod_{i=1}^{r}K_v[x]/(f_i(x))$ 中被映为 $(x+(f_1(x)),\cdots,x+(f_r(x)))$. 因此，对每个 $1\le i\le r$, 映射 $\xi\longmapsto x+(f_i(x))$ 导出了一个由 $K[\xi]$ 到 $K_v[x]/(f_i(x))$ 中的单同

态. 由于 $L=K[\xi]$ 是一个域, 这表明 L 可以嵌入到每个 K_v 的有限扩张 $K_v[x]/(f_i(x))$ 中去. 我们记后面这个域为 L_i. 以 $|\ |_i$ 表示赋值 $|\ |_v$ 在 L_i 上的扩张. 由于 K 在 K_v 中稠密, 故 $K\bigotimes_K L=L$ 在 $K_v\bigotimes_K L$ 中也稠密. 因此 L 在每个 L_i 中稠密. 于是赋值 $|\ |_i$ 在 L 上的限制对应了 L 上的一个位 w_i, 而 L_i 恰为该位对应的完备化 L_{w_i}.

我们还必须证明这些 $|\ |_i$ 都是不同的, 并且它们还是 $|\ |_v$ 在 L 中的所有扩充. 设 $|\ |$ 是在 $|\ |_v$ 中的一个扩张, 则 $|\ |$ 可连续扩充为 $K_v\bigotimes_K L$ 上的一个实值函数, 我们仍记为 $|\ |$, 它应满足性质

$$|\alpha\beta|=|\alpha|\cdot|\beta|,$$

和

$$\begin{cases}|\alpha+\beta|\le\max(|\alpha|,|\beta|), & \text{若}\ |\ |_v\ \text{为非 Archimedes 的},\\ |\alpha+\beta|\le|\alpha|+|\beta|, & \text{若}\ |\ |_v\ \text{为 Archimedes 的}.\end{cases}$$

现在考虑 $|\ |$ 在 L_i 上的限制. 若存在 $\alpha\in L_i$, 使得 $|\alpha|\neq 0$. 则由

$$|\alpha|=|\beta|\cdot|\alpha\beta^{-1}|\neq 0$$

知, 对每个 $\beta\in L_i^\times$, 均有 $|\beta|\neq 0$. 从而 $|\ |$ 在 L_i 上是 $|\ |_i$ 的扩张赋值, 进而由定理 1 知它等于 $|\ |_i$. 由于 $|\ |$ 在 $K_v\bigotimes_K L$ 上非零, 故它一定在某些 L_i 上非零. 这表明所有 $|\ |_v$ 在 L 上的扩充一定在 $\{|\ |_1,\cdots,|\ |_r\}$ 中. 进一步, 如果存在 i 与 j, 使得 $|\ |_i=|\ |_j$, 那么我们取 $|\ |=|\ |_i=|\ |_j$, 这将导出 $|\ |$ 在 L_i 与 L_j 上均非零. 如果将 $\alpha\in L_i^\times$ 和 $\beta\in L_j^\times$ 都视作 $K_v\bigotimes_K L$ 中的元素, 那么在 $K_v\bigotimes_K L$ 中有

$$\alpha\beta=(0,\cdots,\underset{\substack{\uparrow\\ \text{第}\,i\,\text{个}}}{0,\alpha,0},\cdots,0)(0,\cdots,\underset{\substack{\uparrow\\ \text{第}\,j\,\text{个}}}{0,\beta,0},\cdots,0)=(0,\cdots,0)=0.$$

于是 $0=|0|=|\alpha\beta|=|\alpha|\cdot|\beta|\neq 0$, 这是不可能的, 从而证明了定理的代数部分.

剩下来是证明 (2.2) 式也是一个拓扑同构. 对

$$x = (x_1, \cdots, x_r) \in L_{w_1} \bigoplus \cdots \bigoplus L_{w_r},$$

定义

$$\|x\|_0 = \max_{1 \le i \le r} |x_i|_i,$$

则 $\| \ \|_0$ 为 K_v 上向量空间 $L_{w_1} \bigoplus \cdots \bigoplus L_{w_r}$ 的一个范数，它诱导出积拓扑. 另一方面，定理 2 告诉我们，K_v 上有限维向量空间的任意两个范数都是等价的. 于是 $\| \ \|_0$ 诱导出 $K_v \bigotimes_K L$ 上的张量积拓扑. 由此定理得证.

推论 2　设 K 是一个整体域，L 为 K 的有限可分扩张，v 是 K 的一个位，$w_1, \cdots, w_r$ 是位 v 在 L 上的扩张. 设 $\xi \in L$, 则

$$\mathrm{N}_{L/K}(\xi) = \prod_{i=1}^{r} \mathrm{N}_{L_{w_i}/K_v}(\xi),$$

$$\mathrm{Tr}_{L/K}(\xi) = \sum_{i=1}^{r} \mathrm{Tr}_{L_{w_i}/K_v}(\xi).$$

证　与前面的证明相同，我们有

$$\sum_{i=1}^{r} [L_{w_i} : K_v] = n = [L : K].$$

由此，推论对 $\xi \in K$ 成立. 下面我们假定 $\xi \in L$ 且 $K(\xi) = L$. 设 $f(x), f_i(x)$ 与定理 4 证明中的相同，则有

$$\mathrm{N}_{L/K}(\xi) = (-1)^n f(0), \quad \mathrm{N}_{L_{w_i}/K_v}(\xi) = (-1)^{[L_{w_i}:K_v]} f_i(0).$$

以及

$$\mathrm{Tr}_{L/K}(\xi) = -f \text{ 中 } x^{n-1} \text{ 项系数},$$

$$\mathrm{Tr}_{L_{w_i}/K_v}(\xi) = -f_i \text{ 中 } x^{[L_{w_i}:K_v]-1} \text{ 项系数}.$$

由于 $f(x) = f_1(x) \cdots f_r(x)$, 故 ξ 的整体范数与局部范数、整体迹与局部迹的关系恰如推论所言. 最后，假定 $M = K(\xi)$ 是一个中间域，设 $v_1, \cdots, v_s$ 为 M 的所有可整除 v 的位，则 $w_1, \cdots, w_r$ 也

是 L 中可整除某些 v_i 的位. 对 M 的一个固定的位 v_i, 我们有

$$\prod_{w_j|v_i} \mathrm{N}_{L_{w_j}/K_v}(\xi) = \prod_{w_j|v_i} \mathrm{N}_{M_{v_i}/K_v} \mathrm{N}_{L_{w_j}/M_{v_i}}(\xi)$$

$$= \mathrm{N}_{M_{v_i}/K_v}(\xi)^{\sum\limits_{w_j|v_i}[L_{w_j}:M_{v_i}]}$$

$$= \mathrm{N}_{M_{v_i}/K_v}(\xi)^{[L:M]}.$$

从而

$$\prod_{w_j} \mathrm{N}_{L_{w_j}/K_v}(\xi) = \prod_{v_i|v}\prod_{w_j|v_i} \mathrm{N}_{L_{w_j}/K_v}(\xi)$$

$$= \prod_{v_i|v} \mathrm{N}_{M_{v_i}/K_v}(\xi)^{[L:M]}$$

$$= \mathrm{N}_{M/K}(\xi)^{[L:M]} = \mathrm{N}_{L/K}(\xi).$$

同理可证

$$\mathrm{Tr}_{L/K}(\xi) = \sum_{i=1}^{r} \mathrm{Tr}_{L_{w_j}/K_v}(\xi).$$

推论 3 设 K 是一个整体域, L 为 K 的有限可分扩张, v 为 K 的位, $w_1,\cdots,w_r$ 为 L 的可整除 v 的位. 以 $|\ |_v$ 和 $|\ |_{w_i}$ 分别表示 K_v 和 L_{w_i} 的标准赋值. 则对 $\xi \in L$, 有

$$|\mathrm{N}_{L/K}(\xi)|_v = \prod_{i=1}^{r} |\xi|_{w_i}.$$

证明作为练习留给读者.

定理 5 设 K 是一个整体域, $\xi \in K^\times$. 则对几乎所有 K 的位 w, 都有 $|\xi|_w = 1$.

证 当 K 为 $\mathbf{Q}$ 或有限域上单变量有理函数域时, 这是明显的. 若 K 是一个函数域, 但又不是有理函数域时, 可找到一个有理函数子域 F, 使得 K 是 F 的一个有限可分扩张; 若 K 是一个数域, 我们可取 F 为有理数域 $\mathbf{Q}$. 设 $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$ 是 ξ 在 F 上的不可约多项式, 由于对几乎所有的 F 的位 a_i 都是整数, 所以存在一个由有限多个 F 的位构成的集合 S, 使得对所有

在 S 外的 F 的位 v, a_i 均为整数，即 $a_i \in \mathcal{O}_v$. 必要时再扩大一些 S 的范围，我们还可假定对在 S 外所有 F 的位 v, 都有 $|a_0|_v = 1$. 设 $\mathcal{S}$ 是由 K 中那些可整除 S 中某个位的位组成的集合. 由定理 4 知道这个集合 $\mathcal{S}$ 是一个有限集. 对 K 的每个不属于 $\mathcal{S}$ 的位 w, 它整除 F 的一个不含在 S 中的位 v, 这样 ξ 在 $\mathcal{O}_v$ 上整. 从而由定理 2 后的注知它也在 $\mathcal{O}_w$ 中，进而由推论 1 和 3 得

$$|\xi|_w = |\mathrm{N}_{K_w/F_v}(\xi)|_v = |a_0|_v^{[K:F(\xi)]} = 1.$$

这就证明了对所有不在 $\mathcal{S}$ 中的位 w, 有 $|\xi|_w = 1$.

对函数域的情形，上面的定理意味着，对一条定义在有限域上的非奇异射影曲线 C, 定义在 C 上的有理函数只有有限多个零点和极点.

定理 6 (积公式)　设 K 是一个整体域，ξ 为 K 中非零元，则

$$\prod_w |\xi|_w = 1,$$

其中 w 过 K 的所有位，$|\ |_w$ 是关于位 w 的标准赋值.

注　由定理 5 可知，积公式中的无限积 $\prod_w |\xi|_w$ 事实上只是一个有限积，从而这一乘积是有意义的.

证　情形 1：$K = \mathbf{Q}$. 我们可设 $\xi = n$ 是一个非 0 整数，将 n 标准分解为素因子的乘积 $n = \pm p_1^{e} \cdots p_r^{er}$, $e_i > 0$, $p_1, \cdots, p_r$ 为不同的素因子. 当 $i = 1, 2, \cdots, r$ 时，

$$|n|_{p_i} = p_i^{-e_i}.$$

对不是 $\{p_1, \cdots, p_r\}$ 中的任意素数 p, 一定有 $|n|_p = 1$. 此外 $|n|_{\mathbf{R}} = n$, 因此

$$\prod_v |n|_v = 1,$$

其中 v 过 $\mathbf{Q}$ 上所有的位.

情形 2： $K=k(T)$ 是有限域 k 上的有理函数域， k 的势为 q. 设 $\xi=g(T)$ 是 $k(T)$ 中一个多项式，将 $g(T)$ 分解为首一不可约多项式之乘积

$$g(T)=ag_1(T)^{e_1}\cdots g_r(T)^{e_r},$$

其中 $a\in k^\times$, $e_i>0$, $g_1,\cdots,g_r$ 为不同的首一不可约多项式. 以 v_i 表 K 的以 $g_i(T)$ 为局部单值化元素的位，则

$$|g(T)|_{v_i}=q^{-f_ie_i},$$

其中 f_i 是多项式 g_i 的次数. 当 $v\neq v_1,\cdots,v_r,\infty$ 时，同样有

$$|g(T)|_v=1.$$

此外，由于 $g(T)$ 在 ∞ 有一个阶为

$$\deg g=\sum_{i=1}^r f_ie_i$$

的极点，以及 ∞ 是一个次数为 1 的位，所以

$$|g(T)|_\infty=q^{\sum\limits_{i=1}^r f_ie_i}.$$

这就证明了在情形 2 下积公式是正确的.

情形 3： K 是 $F=Q$ 或 $k(T)$ 的有限可分扩张. 设 $\xi\in K^\times$, 则由推论 3 知

$$\prod_{w:K\text{ 的位}}|\xi|_w=\prod_{v:F\text{ 的位}}\prod_{w|v}|\xi|_w=\prod_{v:F\text{ 的位}}|\mathrm{N}_{K/F}(\xi)|_v=1.$$

由此定理成立.

在函数域的情况，上面定理告诉我们，对一条有限域上的非奇异射影曲线 C, 定义在 C 上的非 0 有理函数 ξ 的零点个数与极点个数相同 (包含重数). 这里重数可如下计算：若 ξ 在一个 f 阶闭点 x 处的阶是 e, 则 ξ 在 x 的零点个数为 fe.

推论 4　设 K 是一个常数域为 k 的函数域. 又设 $\xi\in K^\times$, 并且对所有 K 上的位 w, ξ 均含于 $\mathcal{O}_w$ 中，则 ξ 只能是 $k^\times$ 中的元.

证明留作练习.

§3 阿代尔与伊代尔

对一个定义在整体域 K 上的代数群 G, 我们希望知道它的整体解 $G(K)$ 与局部解 $G(K_v)$ 之间的联系. 一个自然的想法是考虑无穷乘积 $\prod_v G(K_v)$ 其中 v 过 K 的所有位. 不幸的是, 这个无穷乘积没有好的拓扑性质. 作为替换, 我们对该乘积加上一些限制条件, 从而引出了"限制直积"的概念.

设 $\{G_v\}_{v\in\Sigma}$ 是一族由集 Σ 参数化的局部紧拓扑群, Σ_0 为 Σ 的一个有限子集. 对任意的 $v\in\Sigma-\Sigma_0$, 我们给定 G_v 的一个紧开子群 H_v. 对 Σ 的每个包含 Σ_0 的有限子集 S, 定义

$$G_S=\prod_{v\in S}G_v\prod_{v\in\Sigma-S}H_v.$$

在该集合上赋予积拓扑, 此时 G_S 仍是局部紧的. 若 S_1 和 S_2 是两个 Σ 的包含 Σ_0 的有限集, 且 $S_1\supset S_2$, 则 $G_{S_1}\supset G_{S_2}$, 并且 G_{S_2} 的拓扑可从 G_{S_1} 的拓扑中诱导出来. $\{G_v\}$ 对于 $\{H_v\}$ 的**限制直积** G 是 G_S 关于 S 在包含映射下的正向极限, 于是

$$G=\left\{x=(x_v)\in\prod_{v\in\Sigma}G_v:\ \text{对几乎所有不在}\,\Sigma_0\,\text{中的}\,v,x_v\in H_v\right\}.$$

设 U 是 G 中的集合, 若对任意包含 Σ_0 的有限集 S, $U\bigcap G_S$ 是开的, 我们则称 U 是 G 中的开集. 由此, 对 G 中单位元的任意一个开邻域, 均可找到包含 Σ_0 的有限集 S, 使得该邻域包含了某个类似于 $\prod_{v\in S}U_v\prod_{v\in\Sigma-S}H_v$ 的集合, 其中 U_v 是 G_v 中含 1 的开子集. 从而 G 是一个局部紧的拓扑群, 且不依赖于 Σ_0 的选择.

习题 20 证明上述断言.

对整体域 K, 设 $\Sigma=\Sigma_K$ 为 K 的位集, $\Sigma_0=\Sigma_\infty$ 为 K 的 Archimedes 位集 (当 K 为函数域时, 该集取为空集). 首先考虑

$G=G_a$ 是加法群的情形. 对任意的 $v\in\Sigma_K$, 令

$$G_v=G(K_v)=K_v.$$

而对 $v\in\Sigma_K-\Sigma_\infty$, 则取

$$H_v=G(\mathcal{O}_v)=\mathcal{O}_v.$$

$\{K_v\}_{v\in\Sigma_K}$ 对于 $\{\mathcal{O}_v\}_{v\in\Sigma_K-\Sigma_\infty}$ 的限制直积关于分量加法及乘法构成一个环, 称为 K 的**阿代尔环**, 记作 A_K. 于是

$$A_K=\left\{(x_v)\in\prod_{v\in\Sigma_K}K_v: \text{对几乎所有的}v, \text{有}\,x_v\in\mathcal{O}_v\right\}.$$

从定理 5 我们知道, K 中元素对几乎所有的位 v 均在 $\mathcal{O}_v$ 中, 于是我们可以将 K 对角地嵌入 A_K 中去.

设 L 是 K 的一个 n 次可分扩张, $\omega_1,\cdots,\omega_n$ 为 L 在 K 上的一组基, v 为 K 的位, $w_1,\cdots,w_r$ 是 L 的可整除 v 的位. 定理 4 告诉我们, 无论在代数上还是在拓扑上, 都有同构

$$K_v\bigotimes_K L=K_v\omega_1\bigoplus\cdots\bigoplus K_v\omega_n\cong L_{w_1}\bigoplus\cdots\bigoplus L_{w_r}.$$

我们希望了解 $\mathcal{O}_v\omega_1\bigoplus\cdots\bigoplus\mathcal{O}_v\omega_n$ 与 $\mathcal{O}_{w_1}\bigoplus\cdots\bigoplus\mathcal{O}_{w_r}$ 之间的关系. 显然, $\mathcal{O}_{w_1}\bigoplus\cdots\bigoplus\mathcal{O}_{w_r}$ 是由 $K_v\bigotimes_K L$ 中在 $\mathcal{O}_v$ 上整的元素构成. 由定理 5 知, 除有限多个位 v 外, $\omega_1,\cdots,\omega_n$ 在 $\mathcal{O}_v$ 上整, 从而 $\mathcal{O}_v\omega_1\bigoplus\cdots\bigoplus\mathcal{O}_v\omega_n$ 含于 $\mathcal{O}_{w_1}\bigoplus\cdots\bigoplus\mathcal{O}_{w_r}$ 中. 反过来, 设 β 是一个 $K_v\bigotimes_K L$ 中在 $\mathcal{O}_v$ 上整的元素, 记

$$\beta=\alpha_1\omega_1+\cdots+\alpha_n\omega_n\in K_v\bigotimes_K L,$$

其中 $\alpha_i\in K_v$. 设 $\sigma_1,\cdots,\sigma_n$ 是 L 到 K 的某个代数闭包 $\overline{K}$ 中的 n 个 K-嵌入, 对 $x=x_1\omega_1+\cdots+x_n\omega_n\in K_v\bigotimes_K L$ 和任意的 $j=1,2,\cdots,n$, 记

$$x^{(i)}=x_1\sigma_i(w_1)+\cdots+x_n\sigma_i(w_n)\in K_v\bigotimes_K\overline{K}.$$

于是由推论 2 可得

$$\sum_{j=1}^{n} x^{(i)} = x_1 \operatorname{Tr}_{L/K}(\omega_1) + \cdots + x_n \operatorname{Tr}_{L/K}(\omega_n)$$

$$= \sum_{j=1}^{n} x_j \sum_{i=1}^{r} \operatorname{Tr}_{L_{w_i}/K_v}(\omega_j)$$

$$= \sum_{i=1}^{r} \operatorname{Tr}_{L_{w_i}/K_v}(x).$$

我们定义 $\operatorname{Tr}_{L/K}(x)$ 为

$$\sum_{i=1}^{n} x^{(i)} = \sum_{i=1}^{r} \operatorname{Tr}_{L_{w_i}/K_v}(x).$$

因此，若 x 在 $\mathcal{O}_v$ 上为整的，一定有 $\operatorname{Tr}_{L/K}(x) \in \mathcal{O}_v$. 由关系

$$\beta = \alpha_1\omega_1 + \cdots + \alpha_n\omega_n$$

导出下面矩阵方程

$$\begin{pmatrix} \omega_1^{(1)} & \cdots & \omega_n^{(1)} \\ \vdots & & \vdots \\ \omega_1^{(n)} & \cdots & \omega_n^{(n)} \end{pmatrix} \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} = \begin{pmatrix} \beta^{(1)} \\ \vdots \\ \beta^{(n)} \end{pmatrix}.$$

又因 $\omega_1, \cdots, \omega_n$ 是 K-线性无关的，所以矩阵 $W = (\omega_j^{(i)})$ 有非 0 行列式. 利用 Cramer 法则可得

$$\alpha_i = \frac{\det B_i}{\det W},$$

其中 B_i 是在 W 中将第 i 列换成 $\begin{pmatrix} \beta^{(1)} \\ \vdots \\ \beta^{(n)} \end{pmatrix}$ 而得到的矩阵. 不过从这里我们并不能了解到 α_i 的很多信息. 但对于

$$\alpha_i^2 = \frac{\det({}^{t}B_iB_i)}{\det({}^{t}WW)}$$

却知道得多一些，这是因为 ${}^tWW = (\mathrm{Tr}_{L/K}(\omega_i\omega_j))$ 是 $\mathcal{O}_v$ 上的矩阵，${}^tB_iB_i$ 亦是如此. 更精细一些，由定理 5 知道 $d = \det({}^tWW)$ 是 K 中的一个非 0 元素，所以对 K 的几乎所有的位 v，均有 $|d|_v = 1$，进而 α_i^2 及 α_i 均在 $\mathcal{O}_v$ 中. 这样我们就证明了，对几乎所有的 K 的位 v，元素 $\beta \in \mathcal{O}_v\omega_1 \bigoplus \cdots \bigoplus \mathcal{O}_v\omega_n$，即

引理 1 设域 L 是整体域 K 的 n 次可分扩张，$\omega_1, \cdots, \omega_n$ 为 L 在 K 上的基，则对 K 的几乎所有的位 v，有

$$\mathcal{O}_v\omega_1 \bigoplus \cdots \bigoplus \mathcal{O}_v\omega_n = \mathcal{O}_{w_1} \bigoplus \cdots \bigoplus \mathcal{O}_{w_r}.$$

结合定理 4 与引理 1 就得到:

引理 2 设域 L 为整体域 K 的 n 次可分扩张，则 $A_K \bigotimes_K L$ 同构于 A_L，并且 $L = K \bigotimes_K L$ 可对角地嵌入到 A_L 中.

下面我们将证明阿代尔环理论中的一个基本结论.

定理 7 设 K 是一个整体域，则加法群 K 是阿代尔环 A_K 的离散子群，且 A_K/K 关于商拓扑是紧的.

证 设 F 是 Q 或有限域 k 上的有理函数域，使得 K 是 F 的有限可分扩张. 设 $n = [K : F], \omega_1 \cdots, \omega_n$ 是 K 在 F 上的基. 则作为加法群有

$$A_K = A_F \bigotimes_F K = A_F\omega_1 \bigoplus \cdots \bigoplus A_F\omega_n.$$

假设我们已证明 F 是 A_F 的一个离散子群，且在 A_F 中存在一个紧子集 Ω，使得 $A_F = F + \Omega$，则 K 也是 $A_F \bigotimes_F K = A_K$ 的离散子群，并且 $A_K = K + \widetilde{\Omega}$，其中 $\widetilde{\Omega} = \Omega\omega_1 + \cdots + \Omega\omega_n$ 亦为 A_K 中的紧子集. 从而 $A_K/K \cong \widetilde{\Omega}/(K \bigcap \widetilde{\Omega})$ 也是紧的. 因此我们只需就 $K = \mathbf{Q}$ 和 $k(T)$ 这两种情况来讨论.

情形 1： $K = k(T)$. 设

$$\Omega = \prod_{v \in \Sigma_K} \mathcal{O}_v,$$

它在 A_K 中是既开又紧的. 对位 v，当 $v \neq \infty$ 时，取 v 的局部单

值化元素 ϖ_v 为在 v 处为 0 的首一不可约多项式; 当 $v=\infty$ 时, 则取 $\varpi_v=1/T$. 对有限位 v, 取在 v 处剩余类域的代表元集 S_v 是 $k[T]$ 中次数小于 $\deg v$ 的多项式集; 对无限位 ∞, 则取 $S_\infty=k$. 这样 K_v 中任意元素 x_v 均可写成系数在 S_v 中, 变数为 ϖ_v 的幂级数

$$x_v=\sum_{i>-\infty}s_i\varpi_v^i,\quad s_i\in S_v.$$

称 $\langle x_v\rangle=\sum\limits_{i<0}s_i\varpi_v^i$ 是 x_v 的极点部分. 对 A_K 中元素

$$x=(x_v)_{v\in\Sigma_K},$$

只有有限多个位 v 使得 $\langle x_v\rangle$ 非 0. 对任意两个不相等的位 v 和 w, 有 $\langle x_v\rangle\in\mathcal{O}_w$. 设

$$r=\sum_v\langle x_v\rangle,$$

则 $r\in K$, 且 $x-r$ 处处为整, 即 $x-r\in\Omega$. 这就证明了 $A_K=K+\Omega$. 进一步, 由推论 4 知 $K\bigcap\Omega=k$ 是有限的, 从而 K 在 A_K 中离散, 且 $A_K/K\cong\Omega/k$ 为紧的.

情形 2： $K=\mathbf{Q}$. 设

$$\Omega=\left[-\frac{1}{2},\frac{1}{2}\right]\prod_p\mathbf{Z}_p.$$

对 $\mathbf{Q}$ 的有限位 p, 选择局部值化元素 $\varpi_p=p$. 取 $S_p=\{0,1,\cdots,p-1\}$ 为 p 处剩余类域的表示集. 对 $\mathcal{O}_p$ 中元 x_v, 同前一样地定义极点部分 $\langle x_p\rangle$. 对 $A_\mathbf{Q}$ 中元素 $x=(x_v)$, 由于对几乎所有的位 p, $\langle x_\mathrm{p}\rangle=0$, 故

$$r=\sum_p\langle x_p\rangle$$

是一个有理数且对任意的 p, $x_p-r\in Z_p$. 这样我们可找到整数 n, 使得 $x-r-n$ 的 Archimedes 分支位于 $[-1/2,1/2]$ 中, 这表明 $A_\mathbf{Q}=\mathbf{Q}+\Omega$. 注意到

$$\left(-\frac{1}{2},\frac{1}{2}\right)\sum_p\mathbf{Z}_p$$

是一个不包含其他有理数的 0 的开邻域，因此 $\mathbf{Q}$ 可作为离散子群嵌入到 $A_{\mathbf{Q}}$ 中，并且

$$A_{\mathbf{Q}}/\mathbf{Q} \cong \left(\mathbf{R}\prod_p \mathbf{Z}_p\right) \Big/ \mathbf{Z} \cong (\mathbf{R}/\mathbf{Z})\prod_p \mathbf{Z}_p$$

是紧的. 由此定理得证.

下面来研究 $G = G_m$ 是乘法群的情况. 同前一样，取 $\Sigma = \Sigma_K$ 和 $\Sigma_0 = \Sigma_\infty$. 对 $v \in \Sigma_K$, 命

$$G_v = G(K_v) = K_v^\times.$$

对 $v \in \Sigma_K - \Sigma_\infty$, 取 $H_v = G(\mathcal{O}_v) = \mathcal{U}_v$. $\{K_v^\times\}$ 对于 $\{\mathcal{U}_v\}$ 的限制直积称为 K 的 **伊代尔群**, 记作 I_K, 即

$$I_K = \left\{(x_v) \in \prod_{v\in\Sigma_K} K_v^\times: \text{ 对几乎所有的} v, x_v \in \mathcal{U}_v\right\}.$$

注意：从代数上看，I_K 是 A_K 的单位群. 但在拓扑上，I_K 的拓扑较 A_K 的诱导拓扑要细.

习题 21 证明 I_K 的自同态 $x \longmapsto x^{-1}$ 关于 A_K 的诱导拓扑是不连续的. 事实上，我们赋予 I_K 的拓扑是使 I_K 成为拓扑群的最弱拓扑.

定理 5 告诉我们，$K^\times$ 可对角地嵌入到 I_K 中. 商群 $I_K/K^\times$ 称为 K 的 **伊代尔类群**. 利用 K 在 v 处完备化 K_v 上的标准赋值 $|\ |_v$, 我们能够定义一个由 I_K 到正实数集 $\mathbf{R}_{>0}^\times$ 的映射 $|\ |$:

$$|x| = \prod_v |x_v|_v, \quad x = (x_v) \in I_K.$$

我们称它为 **范映射**. 由于对几乎所有的位 v, x_v 都是单位，所以上面的乘积只是一个有限积，即范映射的定义是合理的.

习题 22 证明范映射是从 I_K 到乘法拓扑群 $\mathbf{R}_{>0}^\times$ 的一个连续同态，其核 I_K^1 是由范为 1 的伊代尔元素构成的.

对数域 K, 范映射的像是所有的正实数，并且

$$I_K = I_K^1 \times (\mathbf{R}_{>0}^\times)_w \cong I_K^1 \times \mathbf{R}_{>0}^\times,$$

这里 w 是 K 的一个 Archimedes 位，$(\mathbf{R}_{>0}^{\times})_w$ 是 $K^{\times}$ 的一个子群. 当 K 是函数域时，设其常数域是有 q 个元素的有限域 k，范映射 $|\ |$ 的像是由 q 的一个幂 q^n 生成的 $\mathbf{R}_{>0}^{\times}$ 的无限循环群，并且

$$I_K = I_K^1 \times \langle x \rangle \cong I_K^1 \times \mathbf{Z},$$

其中 x 是一个伊代尔，且 $|x| = q^n$.

积公式 (定理 6) 说明 $K^{\times}$ 是 I_K^1 的一个子群，又因 K 是 A_K 的离散子群以及 I_K 的拓扑较 A_K 的诱导拓扑为细，所以 $K^{\times}$ 是 I_K 的，从而也是 I_K^1 的离散子群.

定理 8　设 K 是一整体域，则 $K^{\times}$ 是 I_K^1 的离散子群，且 $I_K^1/K^{\times}$ 关于商拓扑是紧的.

显然，我们只需证第二个断言. 为此先介绍一个几何的结果. 对一个伊代尔 $a = (a_v)$，定义 a 的"界定的超平行体" P_a 为集合

$$P_a = \{x = (x_v) \in A_K : |x_v|_v \le |a_v|_v\}.$$

则 $P_a = aP_1$ 是 A_K 的一个紧子集. 由于 A_K/K 是紧的，若以 $\overline{\mu}_K$ 表示 A_K/K 的 Haar 测度，使得 A_K/K 关于此测度的体积为 1；以 μ_K 表示 A_K 上的一个 Haar 测度，它在 A_K/K 上诱导出 $\overline{\mu}_K$. 则 P_a 关于测度 μ_K 的体积有限，并且

$$\mu_K(P_a) = |a|_K \mu_K(P_1).$$

下面引理是说，若 P_a 的体积充分大，则 P_a 至少包含有 K 中的两个元素.

引理 3　存在常数 $c > 0$，使得对满足 $|a| > 1/c$ 的任意伊代尔 a，有

$$P_a \bigcap K^{\times} \ne \emptyset.$$

证　取 K 的伊代尔 $b = (b_v)$，使得当 v 为非 Archimedes 位时，$b_v = 1$；当 v 为 Archimedes 位时，$b_v = 1/4$. 则

$$P_b - P_b \subset P_1 .$$

假设 $P_a\bigcap K^\times$ 是空集，那么 P_{ab} 与 K 在 A_K 中的任意平移至多有一个公共点. 这是因为，若 y_1, y_2 是 $(x+K)\bigcap P_{ab}$ 中两个不同的点，则 $\alpha=y_1-x$, $\beta=y_2-x$ 是 K 中两个不同的元，且 $\alpha-\beta\in P_{ab}-P_{ab}\subset P_a$. 这与假设 $P_a\bigcap K^\times$ 为空集矛盾. 设 $f, \overline{f}$ 分别为 P_{ab} 和 $(P_{ab}+K)/K$ 的特征函数，则我们有

$$\begin{aligned}\mu_K(P_{ab}) &= \int_{A_K} f(x)\mathrm{d}\mu_K(x) = \int_{A_K/K}\sum_{\alpha\in K} f(x+\alpha)\mathrm{d}\overline{\mu}_K(\overline{x}) \\ &= \int_{A_K/K}\overline{f}(\overline{x})\mathrm{d}\overline{\mu}_K(\overline{x}) \le \int_{A_K/K}\mathrm{d}\overline{\mu}_K(\overline{x}) = 1.\end{aligned}$$

注意，这里用到了“对任意 $x\in A_K$, $(x+K)\bigcap P_{ab}$ 的势总不大于 1 ”这个结论. 于是取 $c=\mu_K(P_b)$, 则有 $c|a|\le 1$. 从而对任意满足 $|a|>1/c$ 的伊代尔 a, $P_a\bigcap K^\times$ 非空.

有了这个引理, 我们即可以证明定理 8. 设 a_0 是范数 $|a_0|>1/c$ 的伊代尔. 对 I_K^1 中任意元 a, 我们有

$$|a^{-1}a_0| = |a_0| > 1/c.$$

于是由引理 3 知，存在非 0 元 $\alpha\in K^\times\bigcap P_{a^{-1}a_0}$, 使得 $\alpha a\in P_{a_0}$. 又因 $\alpha a\in K^\times\cdot I_K^1 = I_K^1$, 所以存在 $\beta\in K^\times$, 使得 $\beta(a\alpha)^{-1}\in P_{a_0}$. 结合这两个讨论，我们有 $\beta\in P_{a_0^2}$. 另一方面， $P_{a_0^2}\bigcap K$ 既是紧的又是离散的，从而是个有限集. 设

$$P_{a_0^2}\bigcap K = \{0, \gamma_1, \cdots, \gamma_s\}.$$

我们已经证明了 $a\alpha\in P_{a_0}$ 和 $(a\alpha)^{-1}\in\bigcup_{i=1}^{s}\gamma_i^{-1}P_{a_0}$. 令

$$B = P_{a_0}\bigcup\left(\bigcup_{i=1}^{s}\gamma_i^{-1}P_{a_0}\right),$$

$$B^* = \{x\in I_K : x, x^{-1} \text{ 均在 } B \text{ 中}\}.$$

我们可以找到 K 的一个的有限位集 S, 使得对任意不在 S 中的 K 的位 v, $(a_0)_v$ 和 $(\gamma_i)_v$ 均是单位，其中 $i=1,2,\cdots,s$. 因此 B^* 是

$\prod_{v\in S} K_v^\times$ 的紧子集与 $\prod_{v\overline{\in} S} \mathcal{U}_v$ 的乘积，从而也是 I_K 的一个紧子集. 于是对任意的 $a \in I_K^1$, 存在 $\alpha \in K^\times$, 使得 $a\alpha \in B^*$. 这就证明了 $I_K^1/K^\times$ 是 $I_K^1 \bigcap B^*$ 的一个商，从而一定是紧的. 定理得证.

下面我们来谈一些定理 8 的应用. 首先考虑 K 为函数域的情况，由 K 的位生成的自由 Abel 群称为 K 的**除子群** $\mathrm{Div}(K)$. 除子 $\mathcal{D} = \sum_v n_v v$ 的次数 $\deg \mathcal{D}$ 定义为 $\sum_v n_v \deg v$. 注意，这里 $n_v \in \mathbf{Z}$, 且对几乎所有的 $v, n_v = 0$. 因此 $\deg \mathcal{D}$ 的定义是合理的. 这样我们就得到了一个从 $\mathrm{Div}(K)$ 到 $\mathbf{Z}$ 的同态-次数映射 $\deg : \mathcal{D} \longmapsto \deg \mathcal{D}$, 其核 $\mathrm{Div}^0(K)$ 是由次数为 0 的除子构成的子群①. 对 $\xi \in K^\times, \xi$ 的除子定义为 $\mathrm{div}\ \xi = \sum_v n_v v$, 其中 n_v 是 ξ 在 v 处的阶. 由定理 5 和定理 6 知，对几乎所有的位 v, 有 $n_v = 0$，以及次数

$$\deg(\mathrm{div}\xi) = \sum_v n_v \deg v = 0.$$

因此 $\mathrm{div}\,\xi \in \mathrm{Div}^0(K)$, 我们称这样的除子为**主除子**. 主除子全体构成一个群, 记作 $\mathrm{Prin}(K)$. 商 $\mathrm{Div}^0(K)/\mathrm{Prin}(K)$ 称为 K 的 Jacobian, 记作 $\mathrm{Jac}(K)$.

对 I_K 中的伊代尔 $x = (x_v)$, 定义

$$\mathrm{div}\, x = \sum_v (\mathrm{ord}_v x_v) v.$$

由于对几乎所有的位 v, x_v 是单位，故 $\mathrm{div}x \in \mathrm{Div}(K)$. 在 $\mathrm{Div}(K)$ 上赋以离散拓扑，则映射 $\mathrm{div} : I_K \to \mathrm{Div}(K)$ 是一个连续同态，且是满射，其核为 $\prod_v \mathcal{U}_v$. 注意到，对 $x \in I_K$ 有

$$|x| = \prod_v |x_v|_v = \prod_v q^{-\mathrm{ord}_v x_v \deg v} = q^{-\deg(\mathrm{div} x)},$$

其中 q 是 K 的常数域的势. 注意到，范数为 1 的伊代尔子群 I_K^1 被 div 满映射为 $\mathrm{Div}^0(K)$, $K^\times$ 则被映为 $\mathrm{Prin}(K)$. 于是 div 诱导了

① 利用 Hecke 的一个定理可以证明次数映射的像是 $\mathbf{Z}$. 它的一个算术证明可参见参考文献 [1]. 此结果我们将在第五章 §4 中予以证明.

一个 (代数及拓扑的) 同构

$$I_K^1 \Big/ \left(K^\times \prod_v \mathcal{U}_v \right) \cong \mathrm{Div}^0(K)/\mathrm{Prin}(K) = \mathrm{Jac}(K).$$

又因 $I_K^1/K^\times$ 是紧的, 所以 $\mathrm{Jac}(K)$ 既是紧的又是离散的, 从而有限, 即

推论 5 设 K 是函数域, 则

$$\mathrm{Jac}(K) = \mathrm{Div}^0(K)/\mathrm{Prin}(K) \cong I_K^1/K^\times \prod_v \mathcal{U}_v$$

是有限的.

下面考虑 K 是数域的情况. 对 K 的每个非 Archimedes 位 v, 以 $\mathfrak{m}_v$ 表 K 的整数环 $\mathcal{O}_K$ 中对应于 v 的极大理想. 以 $\mathcal{F}(K)$ 表示由 $\mathfrak{m}_v$ 生成的自由 Abel 群. $\mathrm{Prin}(K)$ 是由非 0 主理想生成的自由 Abel 群. 由于 $\mathcal{O}_K$ 的任意非 0 理想都是极大理想的积, 且由其阶唯一确定, 故 $\mathrm{Prin}(K)$ 是 $\mathcal{F}(K)$ 的子群. 商群 $\mathcal{F}(K)/\mathrm{Prin}(K)$ 称为 K 的**理想类群** $Cl(K)$.

对一个伊代尔 $x = (x_v) \in I_K^1$, 设 $\vartheta(x)$ 为理想

$$\prod_{v:\,\text{非 Archimedes}} \mathfrak{m}_v^{\mathrm{ord}_v x_v}.$$

由于对几乎所有的 v, x_v 的阶为 0, 所以 $\vartheta(x) \in \mathcal{F}(K)$. 映射 $\vartheta: I_K^1 \to \mathcal{F}(K), x \longmapsto \vartheta(x)$ 是一个群同态. 对 $\mathcal{F}(K)$ 中元

$$\prod_{v:\,\text{非 Archimedes}} \mathfrak{m}_v^{n_v},$$

构造 I_K^1 中伊代尔 $x = (x_v)$ 如下: 在每个非 Archimedes 位 v 处, 选定局部单值化元素 ϖ_v, 命 $x_v = \varpi_v^{n_v}$, 显然对几乎所有的位 v, $x_v = 1$; 再固定一个 Archimedes 位 w, 对所有 $\neq w$ 的 Archimedes 位 v, 命 $x_v = 1$, 又选择 $x_w \in K_w$, 使得

$$\prod |x_v|_v = 1,$$

其中乘积过 K 中所有的位 v. 这样构造的伊代尔 x, 显然满足

$$\vartheta(x) = \prod_{v:\,\text{非 Archimedes}} \mathfrak{m}_v^{n_v}.$$

若赋予 $\mathcal{F}(K)$ 离散拓扑, 则 ϑ 是核为

$$I_\infty^1 \prod_{v:\,\text{非 Archimedes}} \mathcal{U}_v$$

的连续满同态, 其中 I_∞^1 是由 $\prod_{v\in\Sigma_\infty} K_v^\times$ 中满足

$$\prod_{v\in\Sigma_\infty} |x_v|_v = 1$$

的元 $x = (x_v)$ 组成的. 进而 ϑ 映 $K^\times$ 为 $\mathrm{Prin}(K)$, 从而 ϑ 诱导了一个 (代数和拓扑的) 同构

$$I_K^1 \Big/ \left(K^\times I_\infty^1 \prod_{v:\,\text{非 Archimedes}} \mathcal{U}_v \right) \cong \mathcal{F}(K)/\mathrm{Prin}(K) = Cl(K).$$

由于 $I_K^1/K^\times$ 紧致, 这就表明 $Cl(K)$ 为离散且紧致的, 从而有限, 即

推论 6(Minkowski) 设 K 是一个数域, 则

$$Cl(K) = \mathcal{F}(K)/\mathrm{Prin}(K) \cong I_K^1 \Big/ \left(K^\times I_\infty^1 \prod_{v:\,\text{非 Archimedes}} \mathcal{U}_v \right)$$

是有限的.

$K^\times \bigcap I_\infty^1 \prod_{v:\,\text{非 Archimedes}} \mathcal{U}_v$ 中的元称为数域 K 的**单位**. Dirichlet 证明了: 单位群是 K 的单位根群 (这是个有限群) 与一个秩为 $(r_1 + r_2 - 1)$ 的自由 Abel 群的积, 其中 r_1 和 r_2 分别为 K 的实位数和复共轭位数.

对一般的代数群 G, 若它是定义在整体域 K 上的话, 阿代尔

点群 $G(A_K)$ 是 $\{G(K_v)\}_{v\in\Sigma_k}$ 对于 $\{G(O_v)\}_{v\in\Sigma_K-\Sigma_\infty}$ 的限制直积.

参 考 文 献

[1] E. Artin and J. Tate, *Class Field Theory*, Benjamin, New York, 1967.

[2] M. F. Atiyah and I. G. Macdonald, *Introduction to Commutative Algebra*, Addison-Weslery , 1969 (中译本：《交换代数导引》, 科学出版社, 北京, 1982).

[3] J. W. S. Cassels and A. Fröhlich, *Algebraic Number Theory*, Thompson, Washington, 1967.

[4] 戴执中, 《赋值论概要》, 人民教育出版社, 北京, 1981.

[5] S. Iyanaga, *The Theory of Numbers*, North-Holland, Amsterdam-Oxford, 1969.

[6] N. Jacobson, *Lectures in Abstract Algebra* , I, II, III, GTM 30, 31, 32, Springer-Verlag, New York.

[7] S. Lang, *Algebraic Number Theory*, GTM 110, Springer-Verlag, New York, 1986.

[8] O. F. G. Schilling, *The Theory of Valuations*, AMS Math. Surveys, 1950.

[9] B. L. van der Warden, *Algebra*, I, II (中译本：《代数学》, I, II, 科学出版社, 北京, 1963, 1976).

[10] A. Weil, *Basic Number Theory*, Springer-Verlag, New York, 1973.

[11] E. Weiss, *Algebraic Number Theory*, MeGraw-Hill, New York, 1963.

[12] O. Zariski and D. Samuel, *Commutative Algebra*, I, II, GTM 28, 29, Springer-Verlag, New York, 1975.

第四章　Riemann-Roch 定理

§1　限制直积的特征标

我们已经知道拓扑群 G 的特征标是一个从 G 到单位圆 S^1 的连续同态. 以后为了方便起见，我们有时也允许这样的同态可以在非零复数 $\mathbf{C}^{\times}$ 范围内取值，此时称它为**拟特征标**. G 的特征标群 $\widehat{G}$ 称为 G 的**拓扑对偶群**, 我们在其上面可以赋予紧开拓扑如下: 对 G 的任意紧子集 K 和任意的 $\varepsilon > 0$, 设

$$U(K,\varepsilon) = \{\chi \in \widehat{G} : 对任意的 x \in K, |\chi(x) - 1| < \varepsilon\},$$

以 $\{U(K,\varepsilon)\}$ 作为 G 的平凡特征标的开邻域系，则可得到 $\widehat{G}$ 的一个拓扑，即所谓的紧开拓扑. $\widehat{G}$ 关于此拓扑是一个拓扑群.

设 Σ_0 是指标集 Σ 的一个有限子集. 对每个 $v \in \Sigma$, 给定一个局部紧的交换拓扑群 G_v, 而对 $v \in \Sigma - \Sigma_0$, 则取定 G_v 的一个紧开子群 H_v. 在这一节中，我们将研究 $\{G_v\}$ 对于 $\{H_v\}$ 的限制直积 G 的对偶群 $\widehat{G}$. 在此提请读者注意: 通过让其他指标的分量为单位的方式我们可以把 G_v 嵌入到 G 中，从而可以将 G_v 视作 G 的子群. 今后，我们将混用记号 G_v 来表示群 G_v 及其在 G 中的嵌入.

设 χ 是 G 的一个 (拟) 特征标，以 χ_v 表示 χ 在 G_v 上的限制，则 χ_v 也是 G_v 的一个 (拟) 特征标. 对于 χ 和 χ_v, 我们有下面的结论:

命题 1　*对几乎所有的 v, χ_v 在 H_v 上是平凡的. 进而我们有*

$$\chi(a) = \prod_v \chi_v(a_v), \quad a = (a_v) \in G.$$

注　由于对几乎所有的 v, $a_v \in H_v$ 且 χ_v 在 H_v 上平凡，所以

上面的乘积事实上只是一个有限积.

证 设 U 是 1 在 $\mathbf{C}^\times$ 中的一个开邻域，且除 $\{1\}$ 以外不包含其他任何 $\mathbf{C}^\times$ 的子群. 于是 $N=\chi^{-1}(U)$ 是一个 G 的单位元的开邻域. 由 G 上拓扑的定义知道，我们可以找到一个 Σ 的有限集 S，对 $v\in S$，存在 G_v 单位元的开邻域 N_v，使得 N 包含

$$\prod_{v\in S} N_v \prod_{v\in \Sigma-S} H_v.$$

由于 $\chi_v(H_v)$ 是包含在 U 中的子群，所以对所有 $\Sigma-S$ 中的指标 v，χ_v 在 H_v 上是平凡的. 对 $a=(a_v)\in G$，取 S' 是 Σ 的一个包含 S 的有限子集，使得对于任意的 $v\in\Sigma-S'$，有 $a_v\in H_v$. 于是对 $v\in\Sigma-S'$，有 $\chi_v(a_v)=1$ 且

$$\begin{aligned}\chi(a)&=\chi\left(\prod_{v\in S'}a_v\prod_{v\in\Sigma-S'}a_v\right)=\chi\left(\prod_{v\in S'}a_v\right)\\&=\prod_{v\in S'}\chi_v(a_v)=\prod_{v\in\Sigma}\chi_v(a_v).\end{aligned}$$

由此命题得证.

命题 2 若对每个 $v\in\Sigma$，给出 G_v 的一个 (拟) 特征标 χ_v，并且对几乎所有的 v，都有 $\chi_v(H_v)=1$. 那么

$$\chi(a)=\prod_v\chi_v(a_v),\quad a=(a_v)\in G$$

就定义了 G 上的一个 (拟) 特征标 χ.

证 显然 χ 为一个同态. 设 S 是 Σ 的一个有限集，使得对不在 S 中的 v，

$$\chi_v(H_v)=1.$$

又设 S 的势为 s. 对 $\mathbf{C}^\times$ 中 1 的一个开邻域 U，设 V 是 1 的一个开邻域且 $V^s\subset U$. 由于对任意的 $v\in S$，χ_v 是连续的，故存在 G_v

单位元的开邻域 N_v, 使得 $\chi_v(N_v) \subset V$. 从而

$$\chi\left(\prod_{v\in S} N_v \prod_{v\in\Sigma-S} H_v\right) = \prod_{v\in S}\chi_v(N_v) \subset V^s \subset U.$$

又因 $\prod_{v\in S} N_v \prod_{v\in\Sigma-S} H_v$ 是 G 的单位元的一个开邻域, 于是 χ 是连续的, 从而是一个 (拟) 特征标.

由命题 1 和 2, 我们可记 $\chi = \prod_v \chi_v$, 但必须记住, 对几乎所有的 v, 都有 $\chi_v(H_v) = 1$.

用 $\widehat{G_v}$ 表示 G_v 的对偶群, 它也是局部紧的. 对 $v \in \Sigma - \Sigma_0$, 有

$$H_v^{\perp} = \{\chi_v \in \widehat{G_v} : \chi_v(H_v) = 1\} = \widehat{G_v/H_v}.$$

由于 H_v 是开的, 故 G_v/H_v 是离散的, 从而其对偶 $H_v^{\perp}$ 为紧的. 又因为 H_v 是紧的, 所以其对偶 $\widehat{H_v}$ 应为离散的. 从 $\widehat{G_v}$ 到 $\widehat{H_v}$ 的限制映射的核是 $H_v^{\perp}$, 从而 $\widehat{G_v}/H_v^{\perp}$ 同构于 $\widehat{H_v}$ 的一个子群, 故它应为离散的. 这就表明 $H_v^{\perp}$ 是 $\widehat{G_v}$ 的一个紧开子群.

定理 1 $\{\widehat{G_v}\}_{v\in\Sigma}$ 对于 $\{H_v^{\perp}\}_{v\in\Sigma-\Sigma_0}$ 的限制直积 (代数和拓扑) 同构于 G 的对偶群 $\widehat{G}$.

证 为方便起见, 在这里记 $\{\widehat{G_v}\}_{v\in\Sigma}$ 对于 $\{H_v^{\perp}\}_{v\in\Sigma-\Sigma_0}$ 的限制直积为 G^*. 由命题 1 和 2 可知映射

$$(\chi_v) \longmapsto \chi = \prod_v \chi_v$$

是一个从 G^* 到 $\widehat{G}$ 的代数同构, 所以我们只需证明它还是一个拓扑同构, 即我们将证明

$$\chi = \prod_v \chi_v \in \widehat{G}$$

趋近于 G 的平凡特征标的充要条件是 (χ_v) 趋于 G^* 中的单位元. 利用 $\widehat{G}$ 上紧开拓扑的定义, $\chi = \prod_v \chi_v \in \widehat{G}$ 充分靠近 $\widehat{G}$ 的单位元, 即 G 的平凡特征标的充分必要条件是, 存在 G 的一个紧子集

B, 使得 $\chi(B)$ 在 1 的邻近. 不失一般性, 我们假定 B 可以写成

$$\prod_{v\in S} B_v \prod_{v\in \Sigma - S} H_v$$

的形式, 其中 S 是 Σ 的某个有限集, B_v 为 G_v 的紧子集. 而 $\chi(B)$ 与 1 邻近的充要条件是, 当 $v\in S$, $\chi_v(B_v)$ 与 1 接近; 当 $v\in\Sigma-S$ 时, $\chi_v(H_v)=1$(这是因为 $\chi_v(H_v)$ 是一个与 1 非常接近的子群, 而 $\mathbf{C}^\times$ 中只有 $\{1\}$ 是这样的子群). 前者正好等价于在 $v\in S$ 时, χ_v 与 $\widehat{G_v}$ 的平凡特征标接近; 而后者则等价于在 $v\in\Sigma-S$ 时, $\chi_v\in H_v^\perp$. 综合这些讨论, 这就等价于 (χ_v) 与 G^* 中的单位元十分接近, 由此定理得证.

§2 标准加法特征标

在本章的剩余部分, 如无特殊说明, k 总表示一个有 q 个元素的有限域, K 表示常数域为 k 的单变量函数域, $\mathcal{O}_v$ 是局部域 K_v 的整数环. 取定 k 的一个非平凡加法特征标 ϕ. 本节我们的目的是找出 K 的标准加法特征标.

首先研究 $K=k(T)$ 这种情况. 以 ∞ 表示 K 的以 $1/T$ 为局部单值化参数的"无限位". K_∞ 中的元素 x 均可写成

$$x=\sum_{i<\infty} a_iT^i,\quad a_i\in k$$

的形式. K_∞ 上的标准加法特征标 ψ_∞ 定义为

$$\begin{aligned}\psi_\infty(x)&=\psi_\infty(a_nT^n+\cdots+a_0+a_{-1}T^{-1}+\cdots)\\&=\phi(-a_{-1}).\end{aligned}$$

下面将 ψ_∞ 扩充为 $K_\infty\prod\limits_{v\neq\infty}\mathcal{O}_v$ 上的特征标 ψ', 使得 ψ' 在 $\prod\limits_{v\neq\infty}\mathcal{O}_v$

上是平凡的，在 K_∞ 上则是 ψ_∞. 由于

$$\left(K_\infty \prod_{v\neq\infty} \mathcal{O}_v\right) \bigcap K = k[T],$$

以及 ψ' 在 $k[T]$ 上平凡，因此我们可以在

$$K + K_\infty \prod_{v\neq\infty} \mathcal{O}_v$$

上定义特征标 ψ, 使得它在 K 上是平凡的，而在 $K_\infty \prod_{v\neq\infty} \mathcal{O}_v$ 上恰好是 ψ'. 这样，我们就把 ψ' 扩张为 $K + K_\infty \prod_{v\neq\infty} \mathcal{O}_v$ 上的特征标 ψ.

由第三章定理 7 的证明知道

$$A_K = K + K_\infty \prod_{v\neq\infty} \mathcal{O}_v .$$

于是我们构造出在 K 上平凡，在 K_∞ 上的限制是 ψ_∞ 的 A_K 的标准加法特征标 ψ. 当 $v \neq \infty$ 时，用 ψ_v 表示 ψ 在 K_v 上的限制，它是 K_v 的标准特征标.

命题 3 记号同上. 当 $v \neq \infty$ 时，特征标 ψ_v 是 K_v 的一个非平凡的加法特征标，它在 $\mathcal{O}_v$ 上平凡，在 $\mathfrak{p}_v^{-1}$ 上不平凡. 进一步，设 $\pi_v = P_v(T)$ 是在 v 处为 0 的 k 上的首一不可约多项式，则对任意的 $x \in K_v$, 它都可以唯一地写成

$$x = \sum_{i>-\infty} s_i \pi_v^i$$

的形式，其中 $s_i \in k[T]$ 是个次数 $< \deg P_v = \deg v$ 的多项式. 于是

$$\psi_v(x) = \psi_v(s_{-1}\pi_v^{-1}) = \phi(a_{(\deg v)-1}),$$

其中

$$s_{-1} = a_0 + a_1 + a_1 T + \cdots + a_{(\deg v)-1} T^{(\deg v)-1}.$$

证 由定义可知 ψ_v 在 $\mathcal{O}_v$ 上平凡. 又因 ϕ 是 k 的非平凡特征标，所以如果我们证明了 ψ_v 有命题后半部分所描述的性质，那

么 ψ_v 在 $\mathfrak{p}_v^{-1}$ 上是非平凡的. 于是我们所要做的就是计算 ψ_v 在

$$x = s_{-n}\pi_v^{-n} + \cdots + s_{-1}\pi_v^{-1} = \frac{f(T)}{P_v(T)^n}$$

处的值, 其中 s_i 是 $k[T]$ 中次数 $< \deg P_v$ 的多项式, 从而

$$\deg f(T) < \deg P_v(T)^n = \beta.$$

由以前的讨论知, 对所有 $\neq v$ 和 ∞ 的位 w, $f(T)/P_v(T)^n \in \mathcal{O}_w$. 于是

$$1 = \psi\left(\frac{f(T)}{P_v(T)^n}\right) = \psi_\infty\left(\frac{f(T)}{P_v(T)^n}\right)\psi_v\left(\frac{f(T)}{P_v(T)^n}\right).$$

进而得到

$$\psi_v(x) = \psi_\infty\left(-\frac{f(T)}{P_v(T)^n}\right).$$

为确定最后得到的这个值: $\psi_\infty\left(-\frac{f(T)}{P_v(T)^n}\right)$, 命

$$f(T) = T^{\beta-1}(a_{\beta-1} + a_{\beta-2}T^{-1} + \cdots)$$

和

$$P_v(T)^n = T^\beta(1 + b_{\beta-1}T^{-1} + \cdots),$$

于是

$$-\frac{f(T)}{P_v(T)^n} = -T^{-1}(a_{\beta-1} + \mathfrak{p}_\infty \text{ 中元}).$$

由 ψ_∞ 的定义即得

$$\psi_v(x) = \psi_\infty\left(-\frac{f(T)}{P_v(T)^n}\right) = \phi(a_{\beta-1}).$$

很容易验证 $a_{\beta-1}$ 正好是 s_{-1} 中 $T^{(\deg v)-1}$ 项的系数. 由此命题得证.

接下来研究 K 是域 $F = k(T)$ 的有限可分扩张的情形. 我们已经定义了 F 的局部的和整体的标准加法特征标 ψ_v 和 ψ. 现在令 w 是 K 的一个位, v 是 F 的可由 w 整除的位. 我们定义 ψ_w

为 $\psi_v \circ \mathrm{Tr}_{K_w/F_v}$. 由于 $\mathrm{Tr}_{K_w/F_v}(\mathcal{O}_w)$ 是一个含于 $\mathcal{O}_v$ 中的 $\mathcal{O}_v$ 模，故存在整数 $n \geq 0$, 使得它等于 $\mathfrak{p}_v^n$. 这表明，如果 w 不能整除 ∞, 那么 ψ_w 在 $\mathcal{O}_w$ 上平凡；另一方面，由于

$$\mathrm{Tr}_{K_w/F_v}(\pi_v^{-n-1}\mathcal{O}_w) = \mathfrak{p}_v^{-1}$$

和 ψ_v 在 $\mathfrak{p}_v^{-1}$ 上不平凡而知，ψ_w 是 K_w 的一个非平凡特征标. 进一步，利用命题 2 可知这些 ψ_w 定义了 A_K 上的一个特征标

$$\psi = \prod_w \psi_w.$$

利用第三章中的推论 2 则知道 ψ 在 K 上是平凡的. 从而 ψ 是在 K 上平凡的 A_K 的标准特征标. 我们已知道，K_w 中使得

$$\mathrm{Tr}_{K_w/F_v}(x\mathcal{O}_w) \subset \mathcal{O}_v$$

的元素 x 的集合是一个不等于 K_w 的 $\mathcal{O}_w$ 模, 因此存在整数 $d_w \geq 0$, 使得该集合等于 $\mathfrak{p}_w^{-d_w}$. 理想 $\mathcal{D}_w = p_w^{d_w}$ 称做 K_w 在 F_v 上的**共轭差积**(different). 对 K_w 的任意非平凡特征标 η_w, 使 η_w 在 p_w^{-n} 上平凡的最大整数称做 η_w 的阶. 对不能整除 ∞ 位 w, 标准特征标 ψ_w 的阶是 d_w, 而 ψ_∞ 的阶是 -1.

"标准整体加法特征标 ψ 在 K 上是平凡的" 的一个推论是所谓的 "残数定理". 再提醒一下读者，K 的常数域 k 的势是 q. 设 w 是 K 的一个 n 次位使得 k 的剩余类域是 k 的 n 次代数扩张. 从而 K_w 的剩余类域由方程 $x^{q^n} = x$ 在 k 的一个代数闭包中的根组成. 由于 $x^{q^n} = x$ 有 q^n 个不同的根，利用 Hensel 引理知，该方程在 K_w 中也有 q^n 个不同的根. 它们构成了 K_w 中 k 的一个 n 次扩张，记作 k_n. 于是 k_n 是 K_w 的剩余类域在 $\mathcal{O}_w$ 中的代表元集. 进而，对 K_w 的局部单值化参数 π_w, K_w 同构于形式幂级数域 $k_n((\pi_w))$. 对 K_w 中元素 α, 设

$$\alpha = \sum_{i>-\infty} a_i \pi_w^i, \quad a_i \in k_n.$$

定义

$$\mathrm{d}\alpha = \left(\sum_{i > -\infty} i a_i \pi_w^{i-1} \right) \mathrm{d}\pi_w,$$

我们称之为**局部 k-微分**. 容易验证，这种微分具有通常意义下的微分性质. 由这样微分生成的 K_w-模是以 $\mathrm{d}\pi_w$ 为基的一维 K_w 向量空间. 对任意的局部微分 $\omega = f\mathrm{d}\pi_w$, 其中

$$f = \sum_{i > -\infty} a_i \pi_w^i, \quad a_i \in k_n.$$

可以证明系数 a_{-1} 是不依赖于局部单值化参数 π_w 的选择. 从而我们可以定义 ω 在 w 处的残数为

$$\mathrm{Res}_w \omega = a_{-1}.$$

设 $f \in K$. 对由 $\mathrm{d}f$ 这种类型微分生成的 K-模中的元素称做**整体的(亚纯) k-微分**. 这个 K-模是 K 上的一维向量空间，其基可以选成任意一个不为 0 的 $\mathrm{d}f$, 其中 $f \in K$. 设 $f, g \in K$, 整体 k-微分 $\omega = g\mathrm{d}f$ 在 K 的每个位 w 处也是一个局部 k-微分. 又因对几乎所有 K 的位 g 和 f 均为整的，所以只有在有限多个位处 ω 才可能是非全纯的. 令 X 是定义在 k 上的一条非奇异不可约射影曲线，且使得 K 是 X 上的有理函数域. 则存在 k 的一个有限扩张 k_n, 使得 ω 的所有极点都在 $X(k_n)$ 中. 与 Riemann 面上的亚纯微分相类似，我们有:

定理 2(残数定理) 对 $K = k(X)$ 上的任意整体 k-微分 ω, 有

$$\sum_{P \in X(\bar{k})} \mathrm{Res}_P \omega = 0.$$

我们的目的是说明残数定理可以从 ψ 在 K 上的平凡性得到. 首先考虑 $K = k(T)$ 的情形，此时 $X(\bar{k}) = \mathbf{P}^1(\bar{k})$. 我们可将 ω 写成 $f(T)\mathrm{d}T$ 的形式. 将 $f(T)$ 展成其部分分式的和

$$f(T) = \sum_{i=0}^{n} a_i T^i + \sum_{v \neq \infty} \frac{g_v(T)}{P_v(T)^{n_v}}.$$

这里 $a_i \in k$, $P_v(T)$ 是 $k[T]$ 中在闭点 v 处为 0 的首一不可约多项式, $g_v(T)$ 则是 $k[T]$ 中次数小于 $n_v \deg P_v$ 的多项式. 此外, 对几乎所有的 v, 都有 $n_v = 0$. 由于残数是 k 线性的, 于是我们只需就

$$f(T) = T^n, \quad n \geq 0 \quad 和 \quad f(T) = \frac{g_v(T)}{P_v(T)^n}$$

这两种情况来考虑. 当 $f(T) = T^n$ 时, ω 在所有 $\neq \infty$ 的位处是整的. 在 ∞ 位, 取 $\pi_\infty = 1/T$. 于是

$$T = \pi_\infty^{-1}, \quad \mathrm{d}T = -\pi_\infty^{-2} \mathrm{d}\pi_\infty,$$

以及

$$f(T)\mathrm{d}T = \pi_\infty^{-n}(-\pi_\infty^{-2})\mathrm{d}\pi_\infty,$$

它的残数显然是 0; 当

$$f(T) = \frac{g_v(T)}{P_v(T)^n}$$

时, ω 在所有 $\neq \infty, v$ 的位处是整的. 假设 $\deg P_v = r$, 设 $\alpha_1, \cdots, \alpha_r$ 是 $P_v(T)$ 在 $k_r \subset \overline{k}$ 中的根. 与命题 3 一样, 设

$$f(T) = \sum_{i=1}^{n} \frac{s_{-i}}{P_v(T)^i}.$$

进而, 存在常数 $\beta_{ij} \in k_r$, $1 \leq i \leq n$, $1 \leq j \leq r$, 使得

$$f(T) = \sum_{i=1}^{n} \frac{s_{-i}}{P_v(T)^i} = \sum_{i=1}^{n} \sum_{j=1}^{r} \frac{\beta_{ij}}{(T - \alpha_j)^i}.$$

由此看出, $f(T)\mathrm{d}T$ 在 α_j 的残数是 β_{1j}, 而 $\sum\limits_{j=1}^{r} \beta_{1j}$ 正好是 s_{-1} 中 T^{r-1} 项的系数; 在 ∞ 位处, 我们有

$$f(T) = T^{-1}(b_{-1} + b_0 T^{-1} + \cdots),$$

于是

$$f(T)\mathrm{d}T = -(b_{-1}\pi_\infty^{-1} + b_0 + b_1 \pi_\infty + \cdots)\,\mathrm{d}\,\pi_\infty.$$

从而 $f(T)\mathrm{d}T$ 在 ∞ 处的残数是 $-b_{-1}$. 由于 A_K 的标准特征标 ψ 在 K 上平凡, 于是

$$1=\psi(f(T))=\psi_\infty(f(T))\psi_v(f(T))=\phi\left(\sum_{p\in X(\overline{k})}\mathrm{Res}_P f(T)\mathrm{d}\,T\right).$$

由于对任意的 $\alpha\in k$, 特征标 ψ^α 在 K 上也是平凡的, 因而

$$\phi^\alpha\left(\sum_{P\in X(\overline{k})}\mathrm{Res}_P f(T)\mathrm{d}\,T\right)=1.$$

由此就导出

$$\sum_{P\in X(\overline{k})}\mathrm{Res}_P f(T)\mathrm{d}\,T=0.$$

当 K 是 $k(T)$ 的有限可分扩张时, 我们仍记 ω 为 $f\mathrm{d}\,T$, 其中 $f\in K$. 由于总存在 k 的一个有限扩张 k_n, 使得 ω 的极点均在 $X(k_n)$ 中, 所以在必要时扩大常数域, 我们总可假定 ω 的极点全在 $X(k)$ 中. 证明的关键在于: 对 $k(T)$ 的每个位 v, 若 ω 在 K 的位 w 处有极点, 这里 $w|v$, 那么下面关系式成立

$$\sum_{\substack{w|v\\ w:k\text{ 的位}}}\mathrm{Res}_w(\omega)=\mathrm{Res}_v(\mathrm{Tr}_{K/k(T)}\omega):=\mathrm{Res}_v(\mathrm{Tr}_{K/k(T)}f)\mathrm{d}\,T.\quad(2.1)$$

由此, 定理 2 即可由前面关于 $k(T)$ 的讨论得到.

注 残数定理也可写成 X 在 k 上闭点的残数的形式, 即依据 K 的位来写. 事实上, 设 ω 是 K 的一个 k-微分, v 是 K 的一个位, ω 在 v 处的残数位于 v 处的剩余类域 k_v 中, 这里, k_v 在 k 上的扩张次数恰好是 $\deg v$.

定理 2′(残数定理) 设 ω 是 K 的一个 k-微分, 则

$$\sum_{v:K\text{ 的位}}\mathrm{Tr}_{k_v/k}(\mathrm{Res}_v\,\omega)=0.$$

当 $K = k(T)$ 时，同前一样，我们假设 $\omega = f(T)\mathrm{d}T$. 并且在 $v \neq \infty$ 时，

$$f(T) = \frac{g_v(T)}{P_v(T)^n}.$$

于是 $k_v = k_r$ 是 k 的 r 次扩张，位 v 在域 $L = k_r(T)$ 可完全分裂为 r 个 L 的一次位 $\alpha_1, \cdots, \alpha_r$. 假定 ω 在位 v 处可以写成

$$(\cdots + a_{-1}P_v(T)^{-1} + a_0 + \cdots)\,\mathrm{d}\,P_v(T) = \beta\,\mathrm{d}\,P_v(T), \quad a_i \in k_r$$

的形式，那么

$$\mathrm{Res}_v\omega = a_{-1}.$$

由于每个 α_i 是 $P_v(T)$ 的单根，故我们可取 $P_v(T)$ 为域 L_{α_i} 的局部单值化参数. 注意到域 K_v 可以对角地嵌入

$$K_v \bigotimes_k L = L_{\alpha_1} \bigoplus \cdots \bigoplus L_{\alpha_r}$$

中，$\beta \in K_v$ 在 L_{α_i} 中的像等于 β 在 Galois 群 $\mathrm{Gal}(k_v/k)$ 中某个元的作用下的像. 该 Galois 群作用于系数 a_i 上且保持 $P_v(T)$ 不变，这表明 $\sum\limits_{\alpha_i} \mathrm{Res}_{\alpha_i}\omega$ 是 a_{-1} 在 Galois 群 $\mathrm{Gal}(k_v/k)$ 作用下的所有共轭元素之和. 换句话说，它等于

$$\mathrm{Tr}_{k_v/k}(a_{-1}) = \mathrm{Tr}_{k_v/k}(\mathrm{Res}_v\omega).$$

由此定理 2′ 对 $K = k(T)$ 是成立的.

当 K 是 $F = k(T)$ 的有限可分扩张时，对 K 的 k-微分 ω 和 F 的位 v 有

$$\sum_{\substack{w:K\text{的位}\\ w|v}} \mathrm{Tr}_{k_w/k}(\mathrm{Res}_w\,\omega) = \sum_{w|v} \mathrm{Tr}_{k_v/k}\mathrm{Tr}_{k_w/k_v}(\mathrm{Res}_w\,\omega).$$

我们可以证明

$$\mathrm{Tr}_{k_w/k_v}(\mathrm{Res}_w\,\omega) = \mathrm{Res}_v(\mathrm{Tr}_{K_w/F_v}\,\omega). \tag{2.2}$$

于是

$$\sum_{\substack{w:K\text{的位}\\ w|v}} \mathrm{Tr}_{k_w/k}(\mathrm{Res}_w\,\omega) = \mathrm{Tr}_{k_v/k}\left(\sum_{w|v}\mathrm{Res}_v(\mathrm{Tr}_{K_w/F_v}\,\omega)\right)$$

$$= \mathrm{Tr}_{k_v/k}\mathrm{Res}_v\left(\sum_{w|v}\mathrm{Tr}_{K_w/F_v}\,\omega\right)$$

$$= \mathrm{Tr}_{k_v/k}\mathrm{Res}_v(\mathrm{Tr}_{K/F}\,\omega).$$

这样，利用 $\mathrm{Tr}_{K/F}\,\omega$ 是 F 的 k-微分可得：

$$\sum_{w}\mathrm{Tr}_{k_w/k}(\mathrm{Res}_w\,\omega) = \sum_{v:F\text{ 的位}}\sum_{w|v}\mathrm{Tr}_{k_w/k}(\mathrm{Res}_w\,\omega)$$

$$= \sum_{v}\mathrm{Tr}_{k_v/k}\mathrm{Res}_v(\mathrm{Tr}_{K/F}\,\omega) = 0.$$

关于微分和残数定理的更多讨论，读者可以参考 [4]、[6] 和 [8] 等参考文献.

最后我们指出，公式 (2.1) 只是公式 (2.2) 的一种特殊情况.

习题 1 证明存在一个 $A_{\mathbf{Q}}$ 上的且在 $\mathbf{Q}$ 上平凡的加法特征标 ψ，使得 ψ 在 $\prod_{p}\mathbf{Z}_p$ 上平凡，而它在 $\mathbf{R}=\mathbf{Q}_\infty$ 上的限制是

$$\psi_\infty(x) = \mathrm{e}^{-2\pi\mathrm{i}x}.$$

进而，对每个素数 p，给出 ψ 在 $\mathbf{Q}_p$ 上的限制 ψ_p 的表述.

§3 对 偶

设 v 是 K 的位，借助于上节定义的标准加法特征标 ψ_v，我们可以得到 K_v 与其对偶 $\widehat{K}_v$ 之间的同构.

定理 3 映射 $\theta: x \longmapsto \psi_v^x$ 给出了一个由 K_v 到其拓扑对偶 $\widehat{K}_v$ 之间的代数及拓扑同构.

在证明之前，我们先回忆一下有关 ψ_v^x 的一些内容. ψ_v^x 是一个从 K_v 到 S^1 的映射，它把 y 映为 $\psi_v(xy)$. 由于乘 x 的映射是 K_v 加法群的一个连续同态，所以 ψ_v^x 也是 K_v 的一个加法特征标.

现在我们来证明定理 3. 由于 $\psi_v^{x+y} = \psi_v^x\psi_v^y$, 所以映射 θ 是个代数同态. 又由于 ψ_v 是非平凡的，以及当 $x \neq 0$ 时，乘 x 的映射是 K_v 上的满射，所以 ψ_v^x 是平凡特征标的充要条件是 $x = 0$. 这表明 θ 是单射的. 用

$$H = \{\psi_v^x : x \in K_v\}$$

表示 θ 的像, $\overline{H}$ 是 H 在 $\widehat{K}_v$ 中的闭包，那么

$$\overline{H}^{\perp} = \{y \in K_v:\ \text{对所有}\, x \in K_v,\ \ \text{有}\, \psi_v^x(y) = 1\}.$$

又因 ψ_v 是非平凡的，故由 $\psi_v(yK_v) = 1$ 得 $y = 0$. 这表明 $\overline{H}^{\perp} = 0$. 因此 $\overline{H} = \widehat{K}_v$, 从而 H 在 $\widehat{K}_v$ 中稠密.

下面来证 θ 是连续的. 设 V 是 $\mathbf{C}$ 中 1 的一个开邻域. 取 $B = \{x \in K_v : |x|_v \leq M\}$ 是 K_v 的一个紧子集，其中 M 是正常数. 所有将 B 映入 V 的特征标构成了 H 中平凡特征标的一个开邻域 N.

习题 2 对 H 中平凡特征标的任意一个开邻域 W, 总存在一个如上所取的开邻域 N, 使得 $N \subset W$.

由于 ψ_v 是连续的，所以存在正数 δ, 使得所有满足 $|x|_v \leq \delta$ 的元素 $x \in K_v$ 均被 ψ_v 映入 V 中. 取 U 是 K_v 中由满足 $|x|_v < \delta/M$ 的元素 x 组成的 0 的一个开邻域. 则 UB 中元素的赋值 $< \delta$, 故它们被 ψ_v 映入 V 中. 这就说明 $\theta(U)$ 含于 N 中. 结合习题 2 中的结论，我们就证得了 θ 的连续性.

接下来证明 θ^{-1} 的连续性. 给定 $0 \in K_v$ 的开邻域 U, 我们必须找到 K_v 的一个紧子集 B 和 $\mathbf{C}$ 中 1 的开邻域 V, 使得 H 中所有映 B 为 V 的特征标均在 $\theta(U)$ 中. 由于 ψ_v 是非平凡的，所以存在 $x_0 \in K_v$, 使得 $\psi_v(x_0) \neq 1$. 取 V 是 $\mathbf{C}$ 中以 1 为圆心， $|\psi_v(x_0) - 1|$ 为半径的开圆盘. 我们可假定 U 是由 K_v 中赋值 $< \varepsilon$ 的元素组成

的. 设 $|x_0|_v=\delta$. 取 B 是 K_v 中以 0 为球心, $\delta\varepsilon^{-1}$ 为半径的球. 若 $\psi_v^x(B)\subset V$, 即 $\psi_v(xB)\subset V$, 那么, 如果 $x\notin U$, 则 $|x|_v\geq\varepsilon$, 且 xB 包含有 x_0, 而这与 $\psi_v(x_0)\notin V$ 矛盾. 从而我们就证明了 θ^{-1} 的连续性. 进而得到 θ 的双边连续性. 因此 H 是局部紧的, 另外, H 在 $\widehat{K}_v$ 中是闭的, 从而它必须与 $\widehat{K}_v$ 相等. 这就证得了定理 3.

在 $K=k(T)$ 这种情况, 定理 1 是说整体对偶 $\widehat{A}_K$ 同构于 $\{\widehat{K}_v\}$ 对于 $\{\mathcal{O}_v^{\perp}\}$ 的限制直积. 由定理 3 可知, 我们能够用标准加法特征标 ψ_v 将 $\widehat{K}_v$ 与 K_v 等同起来, 且在此对应之下, 当 $v\neq\infty$ 时, $\mathcal{O}_v^{\perp}=\{\psi_v^x:\psi_v(x\mathcal{O}_v)=1\}$ 与 $\mathcal{O}_v$ 也是一样的, 而在 $v=\infty$ 时, $\mathcal{O}_v^{\perp}$ 则与 $\mathfrak{p}_\infty^2$ 相同. 这是因为在 $v\neq\infty$ 时, ψ_v 在 $\mathcal{O}_v$ 上平凡且在 $\mathfrak{p}_v^{-1}$ 上不平凡 (命题 3), 而在 $v=\infty$ 时, 由定义知 ψ_∞ 在 $\mathfrak{p}_\infty^2$ 上平凡, 而在 $\mathfrak{p}_\infty$ 上不平凡. 从而由整体加法特征标 $\psi=\prod\limits_v\psi_v$, 我们得到一个 $\widehat{A}_K$ 与 A_K 之间的代数与拓扑同构. 更精确一些, $\widehat{A}_K=\{\psi^x:x\in A_K\}$, 这个同构恰好就是 $\psi^x\longmapsto x$.

下面假设 K 是 $F=k(T)$ 的 n 次可分扩张. 由第三章引理 2 知, 加法拓扑群 A_K 同构于 $A_F\bigotimes_F K$, 进而同构于

$$\underbrace{A_F\bigoplus\cdots\bigoplus A_F}_{n\text{个}}=A_F^n.$$

于是 $\widehat{A}_K$ 同构于 $\widehat{A_F^n}=\widehat{A_F}^n$. 进而同构于 A_F^n. 因此 A_K 与 $\widehat{A_K}$ 也是代数和拓扑同构的. 另一方面, 由定理 1 知, $\widehat{A_K}$ 与 $\{\widehat{K_w}\}$ 对于 $\{\mathcal{O}_w^{\perp}\}$ 的限制直积同构. 对 F 的一个 $\neq\infty$ 的位 v, 设 w 是 K 的一个可整除 v 的位, 利用在 w 处的标准加法特征标 ψ_w, 借助定理 3, 我们知道 $\widehat{K_w}$ 与 K_w 等同, $\mathcal{O}_w^{\perp}$ 与 $\mathcal{D}_w^{-1}=\mathfrak{p}_w^{-d_w}$ 等同. 这表明 A_K 同构于 $\{K_w\}$ 对于 $\{\mathcal{D}_w^{-1}\}$ 的限制直积. 特别地,

$$\prod_{w|\infty}\mathcal{O}_w\prod_{w\nmid\infty}\mathcal{D}_w^{-1}$$

在 A_K 中既开又紧. 利用 A_K 上拓扑的定义, 这说明对几乎所有的位 w, 都有 $d_w\geq 0$(为了使该集合是开的), 同时对几乎所有的位

w, 也有 $d_w \leq 0$(为了使该集合是紧的), 于是, 对几乎所有的位 w, 有

$$d_w = 0.$$

由这一结论我们可知映射 $x \longmapsto \psi^x$ 给出了从 A_K 到 $\widehat{A_K}$ 的同构. 总结上面讨论, 就有下面结果

定理 4 映射 $x \longmapsto \psi^x$ 给出了从 A_K 到 $\widehat{A_K}$ 的一个代数和拓扑同构. 进一步, 假设 K 是 $F = k(T)$ 的有限可分扩张, 则对几乎所有的 F 的位 v, 扩张 K_w/F_v 的共轭差积是平凡的, 这里 w 为 K 的可整除 v 的位.

推论 1 $K^\perp = \{\psi^\alpha : \alpha \in K\}$. 换句话说, 在由 ψ 建立的从 $\widehat{A_K}$ 到 A_K 的等同之下, $K^\perp$ 与 K 等同.

证 对 $\alpha \in K, \psi^\alpha$ 在 K 上显然是平凡的. 于是 $K^\perp$ 是 $\widehat{A_K}$ 的包含 K 的子群. 由于 A_K/K 是紧的, 所以 $K^\perp = \widehat{A_K/K}$ 为离散的. 于是 $K^\perp/K$ 作为紧群 A_K/K 的一个离散子群一定是有限的. 另一方面, $K^\perp$ 是 K 上的向量空间, K 是无限集, 于是 $K^\perp/K$ 的有限性只能在 $K^\perp = K$ 时才有可能. 由此推论得证.

注 任意一个非平凡的局部的 (或整体的) 加法特征标都可建立从 K_v (或 A_K) 到其拓扑对偶之间的同构. 但在整体对偶的情况, 如果我们还希望 $K^\perp$ 等同于 K 本身, 则还需要该整体加法特征标在 K 上平凡.

§4 Riemann-Roch 定理

首先回顾一下超平行体的定义, 给出 K 的一个伊代尔 $a = (a_v)$, 定义由 a 界定的超平行体为

$$\begin{aligned} P_a &= \{(x_v) \in A_K : \text{对}K\text{的任意位}\, v, \text{有}\ |x_v|_v \leq |a_v|_v\} \\ &= aP_1 = a \cdot \prod_v \mathcal{O}_v. \end{aligned}$$

由于 P_a 是 A_K 的一个紧开子群, K 是 A_K 的一个离散子群, 所

以它们的交 $\Lambda_a = P_a \bigcap K$ 是一个有限群. 进一步, 由于 Λ_a 关于 k 的数乘是封闭的, 因此 Λ_a 是 k 上的有限维向量空间, 记其维数为 $\lambda(a)$, 从而 Λ_a 的势是 $q^{\lambda(a)}$.

同定理 4 一样, 利用标准加法特征标 ψ 把 A_K 与它的对偶 $\widehat{A_K}$ 等同起来. 现在我们来研究 P_a 的对偶

$$P_a^{\perp} = \{x \in A_K : \psi(xP_a) = 1\} = a^{-1} \cdot P_1^{\perp} = a^{-1} \prod_v \mathcal{O}_v^{\perp}.$$

在上一节我们已经证明了, 对所有的位 v, 存在整数 n_v, 使得

$$\mathcal{O}_v^{\perp} = \mathfrak{p}_v^{n_v},$$

其中, 对几乎所有的位 v, 都有 $n_v = 0$, 即 $\mathcal{O}_v = \mathcal{O}_v^{\perp}$. 于是存在一个伊代尔 c, 使得 $P_1^{\perp} = cP_1$. 从而 $P_a^{\perp} = ca^{-1}P_1$ 同样也是一个超平行体, 而且

$$P_a^{\perp} \bigcap K^{\perp} = P_a^{\perp} \bigcap K = \Lambda_{ca^{-1}}$$

的势是 $q^{\lambda(ca^{-1})}$. 另一方面,

$$P_a^{\perp} \bigcap K^{\perp} = (P_a + K)^{\perp} = A_K / \widehat{(P_a + K)}$$

同构于 $A_K/(P_a + K)$. 用 μ 表示 A_K 上的一个 Haar 测度, $\overline{\mu}$ 是 μ 在 A_K/K 上的诱导测度, 则我们有

$$\begin{aligned} q^{\lambda(ca^{-1})} &= |P_a^{\perp} \bigcap K^{\perp}| = |A_K/(P_a + K)| \\ &= \overline{\mu}(A_K/K)/\overline{\mu}((P_a + K)/K). \end{aligned}$$

由 P_a 到 $(P_a + K)/K$ 的自然映射是核为 $P_a \bigcap K = \Lambda_a$ 的满射, 从而

$$\begin{aligned} \overline{\mu}((P_a + K)/K) &= \mu(P_a)/|\Lambda_a| = |a|\mu(P_1)/q^{\lambda(a)} \\ &= q^{-\deg(\operatorname{div} a) - \lambda(a)}\mu(P_1). \end{aligned}$$

取 K_v 上的 Haar 测度 μ_v, 使得 $\mu_v(\mathcal{O}_v) = 1$. 这样我们可选择测度 μ 为 $\prod\limits_v \mu_v$, 于是 $\mu(P_1) = 1$. 至此我们就证明了

$$q^{\lambda(ca^{-1})} = q^{\lambda(a) + \deg(\operatorname{div} a)}\overline{\mu}(A_K/K).$$

这就表明 $\overline{\mu}(A_K/K)$ 是 q 的一个整次幂，记这个幂次是 $g-1$. 为了确定 g 的值，我们取 $a=1$. 注意到 $\lambda(1)=1, \deg(\operatorname{div} a)=0$, 以及

$$q^{\lambda(c)} = q^1 \cdot q^{g-1} = q^g,$$

故 $g = \lambda(c) \geq 0$. 这样我们就证明了：

定理 5 存在一个非负整数 g 和 K 的伊代尔 c, 使得对 K 的任意伊代尔 a, 都有

$$\lambda(a) = \lambda(ca^{-1}) - \deg(\operatorname{div} a) - g + 1.$$

下面我们把这个定理变成通常的 Riemann-Roch 定理的形式. 如果 K 上除子 $\mathcal{D} = \sum n_v v$ 的所有系数 $n_v \geq 0$, 那么称这个除子为**有效的**, 记作 $\mathcal{D} \geq 0$. 借助有效除子，我们更细致地刻画一下 Λ_a:

$$\Lambda_a = \{\alpha \in K : \alpha \in P_a\} = \{\alpha \in K : \alpha a^{-1} \in P_1\}$$
$$= \{\alpha \in K^\times : \operatorname{div} \alpha + \operatorname{div} a^{-1} \geq 0\} \bigcup \{0\}.$$

对除子 $\mathfrak{a} \in \operatorname{Div}(K)$, 定义

$$L(\mathfrak{a}) = \{\alpha \in K^\times : \operatorname{div} \alpha + \mathfrak{a} \geq 0\} \bigcup \{0\}.$$

取一个伊代尔 a, 使得 $\operatorname{div} a^{-1} = \mathfrak{a}$, 则我们有

$$\Lambda_a = L(\mathfrak{a}), \quad \Lambda_{ca^{-1}} = L(\mathcal{K} - \mathfrak{a}),$$

其中 $\mathcal{K} = \operatorname{div} c^{-1}$. 用 $\lambda(\mathfrak{a})$ 表示 $L(\mathfrak{a})$ 在 k 上的维数，则定理 5 可以写成

定理 5′(Riemann-Roch 定理) 存在非负整数 g 和除子 $\mathcal{K} \in \operatorname{Div}(K)$, 使得对任意除子 $\mathfrak{a} \in \operatorname{Div}(K)$, $\lambda(\mathfrak{a})$ 是有限的，且

$$\lambda(\mathfrak{a}) = \lambda(\mathcal{K} - \mathfrak{a}) + \deg \mathfrak{a} - g + 1.$$

取曲线 X, 使得 K 为 X 上的有理函数域，整数 g 恰好是曲线 X 的亏格，我们也称 g 为域 K 的**亏格**. 由伊代尔 c 产生的除子 $\mathcal{K}$ 依赖于将 $\widehat{A_K}$ 与 A_K 等同起来的标准加法特征标 ψ 的选取. 由于对特征标 ψ 的仅有限制是它应在 A_K 上非平凡且在 K 上平凡，利用推论 1 可知，如果 ψ 是一个这样的标准加法特征标，则其他这

样的特征标均可写成 ψ^{α} 的形式，其中 $\alpha \in K^{\times}$. 对应于这样的 ψ^{α}，相当于将 c 换成 $c\alpha^{-1}$，于是对应的除子 $\mathcal{K}$ 正好变为 $\mathcal{K} + \operatorname{div}\alpha$. 因此 $\mathcal{K} + \operatorname{Prin}(K)$ 是由 K 唯一确定的，我们称之为**典范除子类**.

推论 2 $\lambda(\mathcal{K}) = g$, $\deg \mathcal{K} = 2g - 2$.

证 $\lambda(\mathcal{K}) = g$ 是已知的. 为计算 $\deg \mathcal{K}$，只需在定理 5′ 中取 $\mathfrak{a} = \mathcal{K}$ 即可.

推论 3 对任意次数大于 $2g-2$ 的除子 $\mathfrak{a} \in \operatorname{Div}(K)$，有

$$\lambda(\mathfrak{a}) = \deg \mathfrak{a} - g + 1.$$

证 若 $\deg \mathfrak{a} > 2g - 2$，则 $\deg(\mathcal{K} - \mathfrak{a}) < 0$. 对任意 $\alpha \in K$，$\operatorname{div}\alpha + \mathcal{K} - \mathfrak{a}$ 有负的系数，因此它不可能是一个有效除子. 这就表明 $\lambda(\mathcal{K} - \mathfrak{a}) = 0$. 于是 $\lambda(\mathfrak{a}) = \deg \mathfrak{a} - g + 1$.

用伊代尔语言来描述推论 3，即是

推论 4 对任意满足 $\deg(\operatorname{div} a) < 2 - 2g$ 的伊代尔 $a = (a_v) \in I_K$，有

$$A_K = K + P_a = K + \prod_v a_v \mathcal{O}_v.$$

证 此时我们有 $\lambda(ca^{-1}) = 0$，而这正好意味着

$$\overline{\mu}(A_K/K) = \overline{\mu}((P_a + K)/K),$$

进而就导出 $A_K = K + P_a$.

在本节的剩余部分，我们将讨论一下 Riemann-Roch 定理在 K 上全纯微分方面的应用. 给出 K 的一个非零的整体 k-微分 ω. 在 K 的任意一个位 v 处，将 ω 写成 $\alpha d\pi_v$ 的形式，其中 k_v 是 k 的一个有限扩张且同构于 K 在位 v 处的剩余类域，π_v 是 K_v 的局部单值化参数，$\alpha \in k_v((\pi_v))$ 是一个系数在 k_v 中，变量是 π_v 的形式幂级数. 定义 α 在 v 处的阶是 ω 在 v 处的阶，它是不依赖于局部单值化参数 π_v 选取的. 由于存在 K 中两个函数 f 和 g，使得 $\omega = f dg$，所以 ω 只可能在有限多个位处有非零阶，从而和式 $\sum_v (\operatorname{ord}_v \omega) v$ 是 $\operatorname{Div}(K)$ 中的一个除子，我们称之为 ω 的除子，并记

作 $\operatorname{div}\omega$. 当除子 $\operatorname{div}\omega$ 是有效除子时，我们说 ω 是一全纯微分.

设 $K=k(T)$ 是 k 上的有理函数域，ψ 是 A_K 的标准加法特征标. 在上一节我们已经知道

$$P_1^{\perp}=\prod_v \mathcal{O}_v^{\perp}=\mathfrak{p}_\infty^2\prod_{v\neq\infty}\mathcal{O}_v .$$

于是我们可选择伊代尔 c 为 $c_\infty=\pi_\infty^2$, $c_v=1$, 这里 $v\neq\infty$. 从而 $P_1^{\perp}=P_c$. 这样 $\mathcal{K}=\operatorname{div}c^{-1}=-2\infty$ 是 K 的一个典范除子. 接下来考虑微分 $\omega=\mathrm{d}\,T$ 的除子 $\operatorname{div}\omega$. 我们可以证明

$$\operatorname{div}\omega=-2\infty=\mathcal{K}.$$

事实上，在位 $v(\neq\infty)$ 处，取其局部单值化参数 π_v 是在 v 处为 0 且系数在 k 中的首一不可约多项式. 将 T 展成 π_v 的幂级数 $a_0+a_1\pi_v+a_2\pi_v^2+\cdots$, 其中 $a_i\in k_v$, $i=0,1,2,\cdots$, 于是 $\mathrm{d}\,T=(a_1+2a_2\pi_v+\cdots)\mathrm{d}\,\pi_v$. 我们可以断言 $a_1\neq 0$. 如若不然，则 $T\equiv a_0\ (\operatorname{mod}\pi_v^2)$. 设 $r=\deg v$, 再注意到 $a_0\neq 0$, 于是 $T^{q^r-1}\equiv 1\ (\operatorname{mod}\pi_v^2)$, 这表明 π_v^2 可整除 $T^{q^r-1}-1$. 注意到方程 $\chi^{q^r-1}-1=0$ 在 k 的代数闭包 $\bar{k}$ 中是无重根的，所以多项式 $x^{q^r-1}-1$ 在 k 上的因式分解中不可能有平方因子，这就与 π_v^2 可整除 $T^{q^r-1}-1$ 产生矛盾. 从而断言 $a_1\neq 0$ 是正确的. 这说明了，对 $\neq\infty$ 的位 v, $\operatorname{ord}_v\omega=0$; 在位 ∞ 处，取局部单值化参数 $\pi_\infty=1/T$, 我们已经证明过 $\mathrm{d}\,T=-\pi_\infty^{-2}\mathrm{d}\,\pi_\infty$, 从而 $\operatorname{div}\omega=-2\infty$.

下面来讨论域 K 是有理函数域 $F=k(T)$ 的有限可分扩张时的情形. 设 w 为 K 的一个位，v 是 F 的可被 w 整除的位. 以 e_w 表示扩张 K_w/F_v 的分歧指数. 所以当取定局部单值化参数 π_v 和 π_w 后，存在 K_w 中单位 u_w, 使得

$$\pi_v=u_w\pi_w^{e_w} .$$

特别地，当 $e_w=1$ 时，即扩张 K_w/F_v 是非分歧的，我们可取 $\pi_v=\pi_w$. 仍回到一般的情况，将单位 u_w 写成 $k_w(\pi_w)$ 中的幂级数

$$u_0+u_1\pi_w+u_2\pi_w^2+\cdots .$$

在 $v \neq \infty$ 时，我们有

$$\begin{aligned}T &= a_0 + a_1\pi_v + a_2\pi_v^2 + \cdots \\ &= a_0 + a_1 u_w \pi_w^{e_w} + a_2 u_w^2 \pi_w^{2e_w} + \cdots \\ &= a_0 + a_1 u_0 \pi_w^{e_w} + (a_1 u_1 \pi_w^{e_w+1} + a_1 u_2 \pi_w^{e_w+2} + \cdots) \\ &\quad + a_2(u_0 + u_1\pi_w + \cdots)^2 \pi_w^{2e_w} + \cdots;\end{aligned}$$

在 $v = \infty$ 时，则有

$$T = -\pi_{K,\infty}^{-1} = -u_\infty^1 \pi_{K,\infty}^{-e_\infty} = -(u_0^1 \pi_{K,\infty}^{-e_\infty} + u_1^1 \pi_{K,\infty}^{1-e_\infty} + \cdots).$$

于是，当扩张 K_w/F_v 是非分歧时，

$$\mathrm{ord}_v \mathrm{d}T = \mathrm{ord}_w \mathrm{d}T;$$

当扩张 K_w/F_v 是弱分歧时，即 $e_w > 1$ 且 e_w 与 k 的特征 p 互素时，

$$\mathrm{ord}_w \mathrm{d}T = \begin{cases} -(e_w+1), & v = \infty, \\ e_w - 1, & v \neq \infty; \end{cases}$$

当扩张 K_w/F_v 是强分歧时，即 $e_w > 1$ 且 $p|e_w$ 时，若 $v \neq \infty$, 则 $\mathrm{ord}_w \mathrm{d}T \geq e_w$; 若 $v = \infty$, 则 $\mathrm{ord}_w \mathrm{d}T \leq -e_w$.

回忆一下扩张 K_w/F_v 的共轭差积 $\mathcal{D}_w = \mathfrak{p}_w^{d_w}$ 的定义，我们有

$$\mathfrak{p}_w^{-d_w} = \{x \in K_w : \mathrm{Tr}_{K_w/F_v}(x\mathcal{O}_w) \subset \mathcal{O}_v\} \supseteq \mathcal{O}_v.$$

可以证明，扩张 K_w/F_v 是非分歧的充要条件是 $\mathcal{D}_w = \mathcal{O}_w$. 联系到定理 4, 我们发现，对几乎所有的位 w, 扩张 K_w/F_v 都是非分歧的. 进一步，若 K_w/F_v 是弱分歧的，则 $d_w \geq e_w$. 分歧理论更深入的研究表明，作为 K 上的微分，微分 $\mathrm{d}T$ 的除子正好是 $\mathrm{div}\, c^{-1}$, 其中 c 是一个伊代尔且满足 $P_c = \prod_w \mathcal{O}_w^\perp$. 换句话说，即是 $\mathrm{div}\,\mathrm{d}T = \mathcal{K}$.

定理 6 对 K 的任意典范除子 $\mathcal{K}$, 总存在 K 的 k-微分 ω, 使得 $\mathrm{div}\,\omega = \mathcal{K}$. 更进一步，$K$ 上全纯 k-微分集构成了 k 上的 g 维向量空间，这里 g 是 K 的亏格.

证 我们已证明了 $\mathrm{div}\,\mathrm{d}T$ 是 K 的一个典范除子. 由于任意两个典范除子只相差一个主除子，于是我们可选取 K 中适当的函数

f, 使得 $\omega = f\mathrm{d}T$ 就是所需的微分. 此外, 由于 K 上的 k- 微分空间是 K 上的一维空间, 所以对如上给定的微分 ω, 任意一个 K 上的 k- 微分 ω' 均可写成 $\omega' = g\omega$ 的形式; 其中 $g \in K$. 又因微分 ω' 全纯的充要条件为

$$\operatorname{div} \omega' = \operatorname{div} g + \operatorname{div} \omega = \operatorname{div} g + \mathcal{K} \geq 0,$$

而这又等价于 g 在空间 $L(\mathcal{K})$ 中, 利用推论 2 可知 $L(\mathcal{K})$ 的维数为 g, 从而 K 的全纯 k- 微分空间的维数也是 g, 由此定理得证.

对于熟悉 Riemann 面理论的读者而言, 设 C 是使 $K = k(C)$ 成立的代数曲线, 则 K 上的全纯 k- 微分空间的维数恰好是 C 的"几何"亏格, 这是因为它与 C 的几何性态有着密切的联系. 如果我们把 Riemann-Roch 定理中出现的 g 视为 C 的"代数"亏格, 这是因为它的导出完全是代数化的, 那么定理 6 就说明了 C 的"代数"亏格与"几何"亏格是相等的.

Riemann-Roch 定理无疑是数学中最重要的定理之一, 限于本书的目的, 我们不能对此做更多的介绍, 请读者参阅伍鸿熙、吕以辇和陈志华合著的书 [9], 或至少浏览一下其中的引言和每章后的注记, 从而读者可以了解到 Riemann-Roch 定理对数学的意义、影响及其进一步的发展. 此外, 参考文献 [9] 中也有相关的文献介绍. 我们在本章末还列出了一些参考文献, 读者可以从中了解到有关 Riemann-Roch 定理在数论中的应用的更详细的介绍.

§5 有限域上曲线点的个数的计算

在这一节中, k 是一个有 q 个元素的有限域. 设 C 是 k 上的一条亏格为 g 的非奇异射影曲线, p 是 k 的特征. 同样, k_n 表示 k 的 n 次域扩张, $\overline{k}$ 表示 k 的一个代数闭包. 我们用 $\overline{N_n}$ 表示曲线 $C(\overline{k})$ 上 k_n 有理点的个数. 在第二章中我们已讨论了形式幂级数

$$\sum_{n\geq 1} \overline{N}_n U^{n-1} = Z'_C(U)/Z_C(U),$$

其中 $Z_C(U)$ 是曲线 C 的 zeta 函数. Weil 猜想指出 $Z_C(U)$ 可以写成

$$Z_C(U) = \frac{P_1(U)}{(1-U)(1-qU)}$$

的形式, 其中 $P_1(U) = \prod_{i=1}^{2g}(1-\omega_i U)$ 是一个满足函数方程

$$P_1(u) = \pm(q^{\frac{1}{2}}U)^{2g}P_1\left(\frac{1}{qU}\right)$$

次数为 $2g$ 的多项式, 而 $\omega_i (i=1,2,\cdots,2g)$ 是满足 $|\omega_i| = q^{1/2}$ 的复数. 在这一节中, 我们将利用 Riemann-Roch 定理证明关于曲线 C 的 Riemann 猜想, 即 $|\omega_i| = q^{1/2}$. 而关于 C 的 Weil 猜想的其余部分则留到下一章证明. 由于 $P_1(u)$ 的解析性质的证明与 ω_i 的大小无关, 所以我们实际上是在假定函数方程成立的前提下来证明 $|\omega_i| = q^{1/2}$.

作为第二章中的一个练习, 我们已经知道结论 $|\omega_i| = q^{1/2}, i = 1,\cdots,2g$, 等价于

$$|\overline{N}_n - q^n - 1| \le 2gq^{\frac{n}{2}}, \quad n \ge 1.$$

这个不等式可以进一步放宽.

引理 1 $|\omega_i| = q^{\frac{1}{2}}, i = 1,\cdots,2g$ 的充要条件是存在一个常数 $M>0$, 使得对充分大的 n, 有

$$|\overline{N}_{2n} - q^{2n} - 1| \le Mq^n.$$

证 必要性是显然的. 现证充分性, 记 $a_n = \overline{N_n} - q^n - 1$. 由 $Z_C(U)$ 的定义知

$$-a_n = \omega_1^n + \cdots + \omega_{2g}^n, \quad n \ge 1.$$

于是

$$\sum_{n=1}^{\infty} a_{2n}U^{2n} = -\sum_{i=1}^{2g} \frac{\omega_i^2 U^2}{1-\omega_i^2 U^2}.$$

由引理中给出的 a_{2n} 的估计知, 上式左边的幂级数在区域 $|U| < q^{-\frac{1}{2}}$ 中绝对收敛于一个全纯函数. 于是等式右边的有理函数的极

点必须在圆盘 $|U| < q^{-1/2}$ 外，即 $|\omega_i| \le q^{1/2}, i = 1, \cdots, 2g$. 又利用函数方程可得 $|\omega_i| \ge q^{1/2}$, 从而，$|\omega_i| = q^{\frac{1}{2}}, i = 1, 2, \cdots, 2g$. 充分性得证.

我们可假定 q 是一个 p 的充分大的偶次幂. 现在只需证明，作为 q 的函数，

$$\overline{N}_1 = q + O(q^{1/2}).$$

我们将采用 Stepanov 的想法来证明这一点. 设 x_0 是 C 上的一个 k 有理点 (如果需要，我们可把 k 换成它的一个有限扩张以保证 x_0 的存在性). 如果我们能够构造出这样一个 C 上的有理函数 f, 它在 C 的其他 k- 有理点上为 0, 且这些零点的阶均 $\ge m$. 这样 $m(\overline{N}_1 - 1) \le f$ 的零点数 $= f$ 的极点数，进而

$$\overline{N}_1 \le 1 + \frac{1}{m}(f \text{ 极点数}).$$

如果我们还能进一步要求 f 没有太多的极点，则我们就可以得到 $\overline{N}_1$ 的一个好的上界. 它基本上就是

$$\overline{N}_1 = q + O(q^{1/2}).$$

这一有理函数的构造是由 S. A. Stepanov 和 W. Schmidt 独立给出的，但其方法十分相似. 在此我们将采用 Bombieri 在参考文献 [2] 中给出的一个大大简化了的方法.

尽管我们所要研究的是 k 的有限扩张上的问题，但为方便起见，我们将在 k 的代数闭包 $\overline{k}$ 上构造曲线 C 上的有理函数. 此时，Riemann-Roch 定理对这样的有理函数是成立的.

由于域 k 的特征是 p, 其势是 q, 所以 C 上的 k- 有理点都是 Frobenius 态射 $\phi: C(\overline{k}) \to C(\overline{k}), x \longmapsto x^q$ 的不动点. 给出 C 上的一个有理函数 f, $f \circ \phi$ 总可以写成一个有理函数的 q 次幂. 例如，如果 $f(x) = x - a$, 那么

$$f \circ \phi(x) = x^q - a = (x - a^{1/q})^q.$$

于是

$$\operatorname{div}(f \circ \phi) = q \cdot \phi^{-1}(\operatorname{div} f).$$

记

$$\begin{aligned} L_m &= L(mx_0) \\ &= \{f : f \text{ 是 } C(\overline{k}) \text{ 上使得} \operatorname{div} f + mx_0 \geq 0 \text{ 的 } \overline{k}\text{- 有理函数}\} \\ &= \{f : f \text{ 是 } C(\overline{k}) \text{ 上使得} \operatorname{div} f + mx_0 \geq 0 \text{ 的} \\ &\quad k\text{- 有理函数}\} \bigotimes_k \overline{k}. \end{aligned}$$

由于 $\phi(x_0) = x_0$, 于是 $L_m \circ \phi \subseteq L_{qm}$. 又因 ϕ 是满射, 所以 $\dim L_m \circ \phi = \dim L_m$. 对 L_m 和 L_n 的子空间 A 和 B, 我们用 AB 表示由 $fg\,(f \in A,\ g \in B)$ 这样的元素张成的 L_{m+n} 的一个子空间. 命

$$L_m^{(p^\mu)} = \{f^{p^\mu} : f \in L_m\} \subset L_{mp^\mu},$$

显然 $\dim L_m^{(p^\mu)} = \dim L_m$.

引理 2 若 $lp^\mu < q$, 则自然同态:

$$L_l^{(p^\mu)} \bigotimes_{\overline{k}} (L_m \circ \phi) \to L_l^{(p^\mu)}(L_m \circ \phi)$$

是一个同构, 因此 $\dim L_l^{(p^\mu)}(L_m \circ \phi) = (\dim L_l)(\dim L_m)$.

证 由于对任意的 $f, g \in L_{i+1} \setminus L_i$, 总存在常数 $\alpha \in \overline{k}$, 使得 $f - \alpha g \in L_i$, 所以 $\dim L_{i+1} \geq \dim L_i + 1$ (由 Riemann-Roch 定理, 我们知道, 当 $i > 2g-2$ 时, $\dim L_{i+1} = \dim L_i + 1$). 因此, 存在 L_m 的一组基 $s_1, s_2, \cdots, s_r$, 使得 $\mathrm{ord}_{x_0} s_1 < \mathrm{ord}_{x_0} s_2 < \cdots < \mathrm{ord}_{x_0} s_r$. 为证明引理, 我们只需证明: 若存在 $f_i \in L_l, i = 1, 2, \cdots, r$, 且

$$\sum_{i=1}^{r} f_i^{p^\mu} s_i \circ \phi = 0,$$

则 $f_1 = \cdots = f_r = 0$. 如若不然, 设

$$\sum_{i=j}^{r} f_i^{p^\mu} s_i \circ \phi = 0, \quad \text{且 } f_j \neq 0.$$

由于 $\mathrm{ord}_{x_0} f_i^{p^\mu} = p^\mu \mathrm{ord}_{x_0} f_i \geq -lp^\mu$, $\mathrm{ord}_{x_0}(s_i \circ \phi) = q\ \mathrm{ord}_{x_0} s_i$, 以及

在 $s_{i+1},\cdots,s_r$ 中 s_{i+1} 在 x_0 处的阶最小，这样我们得到了

$$\begin{aligned}\mathrm{ord}_{x_0} f_j^{p^\mu} s_j \circ \phi &= \mathrm{ord}_{x_0}\left(-\sum_{i=j+1}^{r} f_i^{p^\mu} s_i \circ \phi\right)\\ &\geq \min_{j+1\leq i\leq r} \mathrm{ord}_{x_0}(f_i^{p^\mu} s_i \circ \phi)\\ &\geq -lp^\mu + q\ \mathrm{ord}_{x_0} s_{j+1}.\end{aligned}$$

这就导出

$$\begin{aligned}p^\mu \mathrm{ord}_{x_0} f_j &\geq -lp^\mu + q(\mathrm{ord}_{x_0} s_{j+1} - \mathrm{ord}_{x_0} s_j)\\ &\geq -lp^\mu + q > 0.\end{aligned}$$

于是 f_j 是一个在 x_0 处为 0 的有理函数，并且它在其余地方没有极点，因此 $f_j = 0$. 而这与假设矛盾. 从而引理得证.

现在我们可以给出 $\overline{N}_1$ 的一个上界.

定理 7 设 $q = p^\alpha$, 其中 α 是一偶数，并且 $q > (g+1)^4$. 则我们有

$$\overline{N}_1 < q + (2g+1)q^{1/2} + 1.$$

证 设 $lp^\mu < q$, 其中 l 和 μ 将在后面明确给出. 利用引理 2 可知，映射

$$\begin{aligned}\delta : L_l^{(p^\mu)}(L_m \circ \phi) &\longmapsto L_l^{(p^\mu)} L_m \subseteq L_{lp^\mu+m},\\ \sum_{i=1}^{r} f_i^{p^\mu}(s_i \circ \phi) &\longmapsto \sum_{i=1}^{r} f_i^{p^\mu} s_i\end{aligned}$$

是一个定义合理的同态. 利用 Riemann-Roch 定理我们有

$$\dim L_i \geq i + 1 - g,$$

并且等号在 $i > 2g+2$ 时成立. 于是再利用引理 2 即得

$$\begin{aligned}\dim\ker\delta &\geq (\dim L_l)(\dim L_m) - \dim L_{lp^\mu+m}\\ &\geq (l+1-g)(m+1-g) - (lp^\mu + m + 1 - g),\end{aligned}$$

其中 $l, m \geq g$. 假设 $\ker\delta \neq \{0\}$, 设 $f = \sum\limits_{i=1}^{r} f_i^{p^\mu}(s_i \circ \phi)$ 是 $\ker\delta$ 中的

非零元. 若 $x \neq x_0$ 是 C 的一个 k-有理点, 则 $\phi(x) = x$, 且

$$\begin{aligned} f(x) &= \sum_{i=1}^{r} f_i(x)^{p^\mu} s_i(\phi(x)) = \sum_{i=1}^{r} f_i(x)^{p^\mu} s_i(x) \\ &= (\delta f)(x) = 0. \end{aligned}$$

这表明, 除了 x_0 点外, f 在 C 的所有其他 k-有理点上均为 0. 更进一步, 由于 $s_i \circ \phi$ 是一个多项式的 q 次幂, 故 f 是个多项式的 p^μ 次幂, 因此 f 至少有 $(\overline{N}_1 - 1)p^\mu$ 个零点. 另一方面, 由于

$$f \in L_l^{(p^\mu)}(L_m \circ \phi) \subseteq L_{lp^\mu + qm},$$

因此它至多有 $lp^\mu + qm$ 个极点.

如果 $lp^\mu < q$, $l, m \geq g$, 以及 $\dim \ker \delta > 0$, 即

$$(l + 1 - g)(m + 1 - g) > (lp^\mu + m + 1 - g),$$

那么

$$\overline{N}_1 \leq 1 + \frac{1}{p^\mu}(lp^\mu + qm) = l + 1 + qm/p^\mu.$$

在 $q = p^\alpha, \alpha$ 是偶数, 以及 $q > (g+1)^4$ 这些条件下, 我们取

$$\mu = \frac{\alpha}{2}, \quad m = p^\mu + 2g = \sqrt{q} + 2g,$$

$$l = \left[\frac{g}{g+1}\sqrt{g}\right] + g + 1,$$

这里 $[x]$ 表示实数 x 的整数部分. 将此代入上面 $\overline{N}_1$ 的不等式就得到所需要的结论. 定理得证.

接下来讲如何用定理 7 导出 $\overline{N}_1 = q + O(q^{\frac{1}{2}})$. 我们知道域 $K = k(C)$ 是有理函数域 $F = k(T)$ 的有限可分扩张. 设 L 是 K 在 F 的一个代数闭包中的 Galois 闭包. 以 C' 表示 k 上的一条非奇异射影曲线, 使得 $L = k(C')$. 这样我们有一个态射列 $C' \to C \to \mathbf{P}^1$, 其中 C' 是 $\mathbf{P}^1$ 的一个 Galois 覆盖, 即域扩张 L/F 是 Galois 扩张, 记其 Galois 群 $\mathrm{Gal}(L/F)$ 为 G. 显然 C' 也是 C 的 Galois 覆盖, 其 Galois 群 H 为 G 的一个子群. C 上的每个 k-有理点都对应了一个 K 的次数为 1 的位. 设 w 是这样的位, 令 v 是 F 的一个可被

w 整除的位. 由于 $k=k_w\supseteq k_v$, 所以 v 也是 F 的次数为 1 的位. 这表明, 在 $C\to\mathbf{P}^1$ 这个态射中, C 上的 k-有理点映到 $\mathbf{P}$ 上的有理点. 我们用 S 表示 $\mathbf{P}^1$ 上的 k-有理点集在 Galois 覆盖 $C'\to\mathbf{P}^1$ 下的原像. 对 $\mathbf{P}^1(k)$ 中的一个点 x, 群 G 可迁地作用在 x 在 C' 中的纤维上, 而 C' 上的 Frobenuis 态射 ϕ 在此纤维上的作用是封闭的, 从而对该纤维上的一点 y, 存在 $\eta\in G$, 使得 $\phi(y)=\eta(y)$. 如果这个 Galois 覆盖在 x 点处是非分歧的话, 那么 x 的纤维中正好有 $|G|$ 个点, 并且上面所述的 η 也是唯一的. 对任意的 $\eta\in G$, 令

$$S(\eta)=\{y\in S:\phi(y)=\eta(y)\}.$$

显然, 当 η 是 G 的单位元时, $S(\eta)$ 正好是 C' 上 k-有理点的集合, 利用证明定理 7 所用的方法, 只需把其中的 δ 换成

$$\delta_\eta: L_l^{(p^\mu)}(L_m\circ\phi)\to L_l^{(p^\mu)}(L_m\circ\eta),$$

我们可得到同样的估计

$$|S(\eta)|\le q+(2g'+1)\sqrt{q}+1,$$

其中 g' 是曲线 C' 的亏格. 另一方面

$$\sum_{\eta\in G}|S(\eta)|=|G||\mathbf{P}^1(k)|+O(1),$$

其中误差项 $O(1)$ 的出现是由于 $\mathbf{P}^1(k)$ 中还有分歧点的缘故. 又因为 $\mathbf{P}^1(k)$ 的势是 $q+1$, 所以结合上面的不等式与等式, 我们就得到了

$$|S(\eta)|=q+O(\sqrt{q}),\quad \eta\in G.$$

容易看出, C 中的点 x 对应了 C' 中的 H-轨道 Hx; 反过来, C' 中一条 H-轨道也对应了 C 中的一个点. 而 C 中的 k-有理点则正好对应了 C' 中的这样一些 H-轨道 Hx, 它们满足 $Hx=H\phi(x)$. 换句话说, 存在 $\eta\in H$, 使得 $\phi(x)=\eta(x)$. 利用前面讨论, 这样的点 x 均在 S 中. 因此, $\bigcup_{\eta\in H}S(\eta)$ 正好是 C' 中这样一些对应了 C

上的 k-有理点的点的集合，于是我们有

$$\sum_{\eta\in H}|S(\eta)| = |H|\overline{N}_1 + O(1).$$

从而得到

$$\overline{N}_1 = q + O(q^{\frac{1}{2}}).$$

这样我们就证明了下面这个定理：

定理 8 设 C 是一条定义在有限域 k 上的亏格为 g 的非奇异曲线. 假设 zeta 函数 $Z_C(u)$ 有下面的形式

$$Z_C(U) = \frac{P_1(U)}{(1-U)(1-qU)},$$

其中 $P_1(u) = \prod_{i=1}^{2g}(1-\omega_i U)$. 再假定 $Z_C(u)$ 满足函数方程

$$Z_C(U) = \pm(q^{\frac{1}{2}}U)^{2g-2}Z_C\left(\frac{1}{qU}\right).$$

则对任意的 $i = 1, 2, \cdots, 2g$, 有

$$|\omega_i| = q^{\frac{1}{2}}.$$

换句话说，就是关于曲线 C 的 "Riemann 猜想" 成立.

参 考 文 献

[1] E. Artin, *Algebraic Number and Algebraic Functions*, Gordon and Breach, New York, 1967.

[2] E. Bombieri, *Counting points on curves over finite fields*, [d'après S. A. Stepanov], Lec. Notes in Math. 383, 234~241, Springer-Verlag, Berlin, 1974.

[3] P. M. Cohn, *Algebraic Numbers and Algebraic Functions*, Chapman and Hall, London, 1991.

[4] M. Eichler, *Introduction to Algebraic Number and Algebraic Functions*, Academic, New York, 1966.

[5] S. Iyanaga, *The Theorg of Numbers*, North-Holland, Amsterdam-Oxford, 1969.

[6] J.-P. Serre, *Algebraic Groups and Class Fields*, GTM 117, Springer-Verlag, New York, 1988.

[7] J. Tate, *Fourier analysis in number fields and Hecke's zeta-functions*, Thesis, Princeton University, 1950, Published in *Algebraic Number Theory*, edited by J. W. S. Cassels and A Fröblich, Thompson, Washington D. C., 1967, republished by Academic Press, London, 1989.

[8] A. Weil, *Basic Number Theory*, Springer-Verlag, Berlin, 1973.

[9] 伍鸿熙、吕以辇、陈志华，《紧黎曼曲面引论》，科学出版社、北京，1983.

第五章　Zeta 函数和 L-函数

在这一章中，我们将讨论射影曲线的 zeta 函数与伊代尔类特征标的 L-函数的解析性质，如解析开拓、函数方程等等.

§1　伊代尔类特征标的 L-函数

首先，如无特殊说明，我们总假定 k 是一个有 q 个元素的有限域， K 是常数域为 k 、亏格为 g 的函数域.

我们知道，伊代尔群 I_K 的拟特征标是一个由 I_K 到 $\mathbf{C}^\times$ 的连续同态，若它还在 $K^\times$ 上是平凡的，则称之为**拟伊代尔类特征标**.

例　对任意伊代尔 $x = (x_v) \in I_K$，定义赋值 $|\ |$ 为

$$|x| = \prod_v |x_v|_v.$$

由第三章 §3 的讨论知， $|\ |$ 是一个 I_K 的拟特征标. 又利用积公式知，它还是一个拟伊代尔类特征标. 于是对任意复数 s，$|\ |^s$ 也是一个拟伊代尔类特征标.

下面这个命题解释了伊代尔群 $I_K/K^\times$ 的拟特征标与特征标之间的关系.

命题 1　*设 χ 是伊代尔类群 $I_K/K^\times$ 的拟特征标，则存在复数 s，使得 $\chi_1 = \chi|\ |^s$ 为 $I_K/K^\times$ 的特征标.*

证　先回忆一下将伊代尔 x 映为 $\deg(\operatorname{div} x)$ 的次数映射

$$\deg \operatorname{div} I_K \to \mathbf{Z}$$

的性质. 我们看到拟特征标 $|\ |$ 可以写成下面形式

$$|x| = q^{-\deg \operatorname{div} x}, \quad x \in I_K.$$

I_K 在次数映射 deg div 下的像是一个无限循环群，设其生成元为 r(事实上，我们将在 §4 看到 $r=1$, 即 deg div 是一个满射). 设 x_0 是一个次数 $\deg(\operatorname{div} x_0)=r$ 的伊代尔. 取复数 s, 使得

$$\chi(x_0)=|x_0|^{-s},$$

则 $\chi_1=\chi|\ |^s$ 是 $I_K/K^\times$ 的一个拟特征标，且它在 x_0 生成的无限循环群 $\langle x_0\rangle$ 上是平凡的. 我们已经知道 deg div 的核是 I_K^1, 换句话说， $I_K=I_K^1\langle x_0\rangle$, 于是 χ_1 在 I_K 上的值群是 $\chi_1(I_K^1/K^\times)$. 然而，由第三章中的定理 8 知， $I_K^1/K^\times$ 是紧的. 这表明， χ_1 的像一定要在单位圆 S^1 上，从而 χ_1 是 $I_K/K^\times$ 的一个有限阶特征标.

在上一章 §1 中我们已经知道，如果 χ 是 I_K 的一个拟特征标，那么，对几乎所有的位 v 处， χ_v 在 $\mathcal{U}_v$ 是平凡的. 假如在位 v 处， χ_v 在 $\mathcal{U}_v$ 上不平凡，则它在 1 的某个邻域 $1+\mathfrak{p}_v^{n_v}$ 中平凡. 满足这一条件的最小正整数 n_v 称为 χ_v 的前导子的**指数**, 此时，我们称 χ 和 χ_v 在位 v 处**分歧**; 假如在位 v 处， χ_v 在 $\mathcal{U}_v$ 上平凡，则取 $n_v=0$, 此时称 χ 和 χ_v 在位 v 处**非分歧**. 于是

$$f(\chi)=\sum_v n_v v$$

定义了 K 的一个除子，我们称为 χ 的**前导子**(conductor).

习题 1 描述 $I_K/K^\times$ 的所有非分歧特征标，并证明它们的全体构成了一个同构于 $\operatorname{Jac}(K)\times S^1$ 的群.

如果在位 v 处，χ 是非分歧的，那么 χ_v 由它在局部单值化元素 π_v 的值决定，并且 $\chi_v(\pi_v)$ 不依赖于 π_v 的选取. 于是我们可以定义:

$$L(s,\chi_v)=(1-\chi_v(\pi_v)\mathrm{N}\,v^{-s})^{-1},$$

其中 $\mathrm{N}\,v=q^{\deg v}$ 是 K_v 的剩余类域的势; 如果在位 v 处 χ 是分歧的，取 $L(s,\chi_v)=1$. 这样，定义 $L(s,\chi)$ 为

$$L(s,\chi)=\prod_v L(s,\chi_v), \tag{1.1}$$

我们称之为拟特征标为 χ 的 L-函数. 容易验证, 对任意的 $s_0 \in C$,

$$L(s, \chi|\ \ |^{s_0}) = L(s + s_0, \chi).$$

于是利用命题 1 可知, 我们总可假定 χ 是一个伊代尔类群的特征标. 下面我们将在此假定下来研究 L-函数 $L(s,\chi)$ 的解析性质.

设 C 是一条非奇异射影曲线, 使得 K 是 C 的 k-有理函数域 (参见第二章); 又设 $Z_C(U)$ 是结合 C 的 zeta 函数, 当 χ 为 $I_K/K^\times$ 的平凡特征标 χ_0 时,

$$L(s, \chi_0) = \prod_v (1 - \mathrm{N}\, v^{-s})^{-1} = Z_C(q^{-s}).$$

此时, 也可以用 $\zeta_K(s)$ 来表示 $L(s,\chi_0)$. 利用无穷乘积知识, 从上式可以看出 $L(s,\chi_0)$ 在 $\mathrm{Re}\, s \gg 0$ 时是绝对收敛的, 于是对 $I_K/K^\times$ 的任意特征标 χ, $L(s,\chi)$ 在某一右半平面上绝对收敛于一个全纯函数, 并且, 当 $\mathrm{Re}\, s \to \infty$ 时, $L(s,\chi) \to 1$. 本章的目的是证明下面两个定理:

定理 1 设 C 是有限域 k 上亏格为 g 的非奇异射影曲线, 它的 zeta 函数 $Z_C(U)$ 可以用 Euler 积

$$Z_C(U) = \prod_v (1 - U^{\deg v})^{-1}$$

来定义, 其中乘积中的 v 过所有 C 的 k 闭点. 当 $|U| < q^{-1}$ 时, 该 Euler 积绝对收敛于一个全纯函数, 事实上, 它是一个有下面形式的有理函数:

$$Z_C(U) = \frac{P_1(U)}{(1-U)(1-qU)},$$

这里 $P_1(U)$ 是一个次数为 $2g$ 的整系数多项式, 并且它还满足关系

$$P_1(U) = (q^{\frac{1}{2}}U)^{2g} P_1\left(\frac{1}{qU}\right),$$

以及 $P_1(0) = 1$ 和 $P_1(1) = h = |\mathrm{Jac}(K)|$.

注 将定理 1 和第四章中的定理 8 结合在一起, 就肯定了关于曲线 C 的 Weil 猜想.

定理 2 设 χ 是伊代尔类群 $I_K/K^\times$ 的一个特征标，且对任意的 $t\in C$, 都有 $\chi\neq|\ |^t$. 那么由上面 Euler 积 (1.1) 定义的 L-函数 $L(s,\chi)$ 在 $\mathrm{Re}\, s>1$ 时绝对收敛于一个整函数. 更精确地讲，存在一个满足 $P(0,\chi)=1$ 和满足函数方程

$$P(U,\chi)=c(\chi)(q^{\frac{1}{2}}U)^{2g-2+\deg\mathfrak{f}(\chi)}P\left(\frac{1}{qU},\chi^{-1}\right)$$

的次数为 $2g-2+\deg\mathfrak{f}(\chi)$ 的多项式 $P(U,\chi)$, 使得

$$L(s,\chi)=P(q^{-s},\chi).$$

或等价地

$$L(s,\chi)=c(\chi)q^{\left(\frac{1}{2}-s\right)(2g-2+\deg\mathfrak{f}(\chi))}L(1-s,\chi^{-1}),$$

其中，$\mathfrak{f}(\chi)$ 是 χ 的前导子，$c(\chi)$ 是一个常数.

若以 $\mathfrak{A}(I_K)$ 表示伊代尔类群的拟特征标群，则在 $\mathfrak{A}(I_K)$ 上可以赋以解析结构，使得任意拟特征标 χ 所在的连通分支是由 $\chi|\ |^s$, $s\in\mathbf{C}/\frac{2\pi\mathrm{i}}{\log q}\mathbf{Z}$ 组成，于是，我们可以用 $I_K^1/K^\times$ 的特征标来参数化 $\mathfrak{A}(I_K)$ 的连通分支. 由于 $\mathbf{C}/\frac{2\pi\mathrm{i}}{\log q}\mathbf{Z}$ 是一个柱面，把它同拟特征标的连通分支等同起来，从而前面定义的 L-函数可以视作是一个定义在 $\mathfrak{A}(I_K)$ 的每个连通分支的某一右半柱面上的拟特征标的整函数. 定理 1 和定理 2 是说，作为一个拟特征标的函数，这个 L-函数可以亚纯延拓到整个流形 $\mathfrak{A}(I_K)$ 上，并且除了在平凡特征标 χ_0 的连通分支中，在 χ_0 和 $\chi_0|\ |$ 处可能有单极点外，这个 L-函数处处全纯. 此外，它还满足函数方程

$$L(\chi)=\tilde{c}(\chi)L(|\ |\chi^{-1}),$$

其中 $\tilde{c}(\chi)$ 是一个定义在 χ 的连通分支上的指数函数.

§2 Fourier 变换

按照 J. Tate 的博士论文[3] 的思想 (也可以参阅参考文献 [1],

[2]), 我们将借助于阿代尔群上的 Fourier 分析来证明定理 1 和定理 2, 在这一节中我们先做些准备.

设 $\mathrm{d}x$ 是阿代尔环 A_K 上的一个加法 Haar 测度, $\overline{\mathrm{d}x}$ 是它在 A_K/K 的上的诱导测度, 并且 A_K/K 关于此测度的体积是 1. 用 ψ 表示在第四章的 §2 中定义的 A_K 的标准加法特征标. 于是利用 ψ, 我们可以把 A_K 与其对偶 $\widehat{A_K}$ 等同起来.

我们称定义在 A_K 上且有紧支集的局部常值函数为 **Schwatz 函数**. Schwatz 函数全体构成了一个线性空间, 记作 $\mathcal{S}(A_K)$. 我们将要研究这些 Schwatz 函数的 Fourier 变换.

习题 2 证明 Schwatz 函数空间 $\mathcal{S}(A_K)$ 可以由平行多面体平移 $x+P_a$ 的特征函数生成, 其中 $x\in A_K, a\in I_K$.

利用已选取好的测度 $\mathrm{d}x$, 对 Schwatz 函数 $\Phi\in\mathcal{S}(A_K)$, 定义它的 Fourier 变换 $\widehat{\Phi}$ 为

$$\widehat{\Phi}(\eta)=\int_{A_K}\Phi(x)\eta(x)\mathrm{d}x,\quad \eta\in\widehat{A}_K.$$

由于 $\widehat{A}_K\cong A_K$, 我们可以把 $\widehat{\Phi}$ 视为 A_K 上的函数:

$$\widehat{\Phi}(y)=\widehat{\Phi}(\psi^y)=\int_{A_K}\Phi(x)\psi^y(x)\mathrm{d}x$$

$$=\int_{A_K}\Phi(x)\psi(yx)\mathrm{d}x,\quad y\in A_K.$$

命题 2 (1) Schwartz 函数的 Fourier 变换仍为一个 Schwartz 函数.

(2) 设 $\Phi\in\mathcal{S}(A_K)$, 则对任意 $x\in A_K$, 有

$$\widehat{\widehat{\Phi}}(x)=\Phi(-x).$$

证 (1) 不失一般性, 我们可设 $\Phi\in\mathcal{S}(A_K)$ 是某个 x_0+P_a 的

特征函数，其中 $x_0 \in A_K, a \in I_K$，则

$$\begin{aligned}\widehat{\Phi}(y) &= \int_{A_K} \Phi(x)\psi(yx)\mathrm{d}x \\ &= \int_{P_a} \Phi(x_0+x)\phi(y(x_0+x))\mathrm{d}x \\ &= \psi(yx_0)\int_{P_a}\psi(yx)\mathrm{d}x.\end{aligned}$$

又由于

$$\int_{P_a}\psi(yx)\mathrm{d}x = \begin{cases}\mathrm{vol}(P_a), & \text{若 } y \in P_a^{\perp}, \\ 0, & \text{若 } y \notin P_a^{\perp},\end{cases}$$

以及 ψ 为局部常值函数，所以 $\widehat{\Phi}$ 显然是个 Schwartz 函数.

(2) 对 $\Phi \in \mathcal{S}(A_K)$，由 (1) 知 $\widehat{\Phi} \in \mathcal{S}(A_K)$. 假设 Φ 和 $\widehat{\Phi}$ 的支集分别含于 P_a 和 P_b 之中. 对任意的 $z \in A_K$，由定义可知

$$\begin{aligned}\widehat{\widehat{\Phi}}(z) &= \int_{P_b}\widehat{\Phi}(y)\psi(yz)\mathrm{d}y \\ &= \int_{P_b}\int_{P_a}\Phi(x)\psi(xy)\psi(yz)\mathrm{d}x\,\mathrm{d}y \\ &= \int_{P_a}\Phi(x)\int_{P_b}\psi((x+z)y)\mathrm{d}y\,\mathrm{d}x.\end{aligned}$$

现取 P_a 足够大，使得 $P_b^{\perp}$ 含于 P_a 之中. 这样，若 $z \notin P_a$，则 $x+z \notin P_b^{\perp}$，从而在 P_b 上的积分为 0，即 $\widehat{\widehat{\Phi}}(z)=0$；若 $z \in P_a$，除非 $x \in -z+P_b^{\perp}$，否则在 P_b 上的积分仍为 0；当 $x \in -z+P_b^{\perp}$ 时，在 P_b 上的积分恰为 P_b 的体积. 于是对 $z \in P_a$

$$\widehat{\widehat{\Phi}}(z) = \mathrm{vol}(P_b)\int_{-z+P_b^{\perp}}\Phi(x)\mathrm{d}\,x.$$

进一步假设 P_b 足够大，使得 Φ 在 $-z+P_b^{\perp}$ 上为常数. 从而，当 $z \in P_a$ 时，

$$\widehat{\widehat{\Phi}}(z) = \mathrm{vol}(P_b)\mathrm{vol}(P_b^{\perp})\Phi(-z) = \Phi(-z)\mathrm{vol}(P_1)\mathrm{vol}(P_1^{\perp}).$$

在第四章 §4 中我们已经证明了 $\mathrm{vol}(A_K/K) = q^{g-1}\mathrm{vol}(P_1)$, 又由 $\mathrm{d}x$ 的选取知 $\mathrm{vol}(A_K/K) = 1$, 于是 $\mathrm{vol}(P_1) = q^{1-g}$. 再由第四章 §4 中推论 2 知

$$\deg \mathrm{div}\, c^{-1} = \deg \mathcal{K} = 2g - 2,$$

于是

$$\mathrm{vol}(P_1^{\perp}) = \mathrm{vol}(P_c) = |c|\mathrm{vol}(P_1) = q^{2g-2}q^{1-g} = q^{g-1}.$$

总结上面讨论, 我们就得到了 $\widehat{\widehat{\Phi}}(z) = \Phi(-z)$, $z \in A_K$. 所以命题得证.

由于有性质 (2), 所以我们说 $\mathrm{d}x$ 是自对偶的. 这一测度被称为 A_K 的玉河 (Tamagawa) 测度.

如果用 Φ_a 来表示 P_a 的特征函数, 由上面的证明可知, $\widehat{\Phi}_a$ 等于 $|a|q^{1-g}$ 乘以 $P_a^{\perp}$ 的特征函数. 注意到

$$P_a^{\perp} = P_{ca^{-1}}, \quad |c^{-1}| = q^{2-2g},$$

以及 P_c 的特征函数可以写作 $\Phi_1(c^{-1}x)$, 从而我们得到:

推论 1 设 Φ_a 表示平行多面体 P_a 的特征函数, 则

$$\widehat{\Phi}_a = |a|\,|c^{-1}|^{1/2}\,\Phi_{ca^{-1}},$$

其中 c 为使得 $P_1^{\perp} = P_c$ 成立的任意伊代尔. 特别地

$$\widehat{\Phi}_1(x) = |c^{-1}|^{1/2}\Phi_1(c^{-1}x), \quad x \in A_K.$$

从命题 2 的证明我们还可推出下面结论.

推论 2 设 Φ 为 $x_0 + P_a$ 的特征函数, 则

$$\widehat{\Phi} = \psi^{x_0}\widehat{\Phi}_a = |a|\,|c^{-1}|^{1/2}\psi^{x_0}\Phi_{ca^{-1}}.$$

对 A_K 上的 Schwartz 函数 Φ, 由于它有紧支集, 又由于 K 是离散的, 所以对任意的 $x \in A_K$, 和式 $\sum\limits_{\alpha\in K}\Phi(x+\alpha)$ 事实上只是一个有限和, 从而可以定义函数:

$$h_{\Phi}(x) = \sum_{\alpha\in K}\Phi(x+\alpha), \quad x \in A_K/K.$$

显然 h_Φ 是一个局部常值函数. 由于 A_K/K 的对偶

$$\widehat{A_K/K} = K^\perp = \{\psi^\beta : \beta \in K\} \cong K,$$

定义 h_Φ 的 Fourier 变换为

$$\widehat{h}_\Phi(\beta) = \widehat{h}_\Phi(\psi^\beta) = \int_{A_K/K} h_\Phi(x)\psi(\beta x)\overline{\mathrm{d}\,x},$$

其中 $\overline{\mathrm{d}\,x}$ 是由 A_K 的玉河测度 dx 诱导出的 A_K/K 上的测度. 从而 $\widehat{h}_\Phi$ 是一个 $\widehat{A_K/K}$ 上的函数. 利用 h_Φ 的定义以及 ψ 在 K 上平凡这一事实, 我们有

$$\begin{aligned}\widehat{h}_\Phi(\beta) &= \int_{A_K/K} \sum_{\alpha\in K} \Phi(x+\alpha)\psi(\beta(x+\alpha))\overline{\mathrm{d}\,x} \\ &= \int_{A_K} \Phi(x)\psi(\beta x)\mathrm{d}\,x = \widehat{\Phi}(\beta).\end{aligned}$$

又因 $\widehat{\Phi}$ 有紧支集, 所以存在平行体 P_b, 使得当 $\beta \notin K \bigcap P_b$ 时, $\widehat{h}_\Phi(\beta) = 0$. 我们把 $\widehat{h}_\Phi(\beta)$ 视作 h_Φ 的 Fourier 系数, 从而有下面结论.

命题 3 (**Fourier反演公式**) 设 Φ 是 A_K 上的 Schwartz 函数, 如上定义 h_Φ, 则

$$h_\Phi(x) = \sum_{\beta\in K} \widehat{h}_\Phi(\beta)\psi(-\beta x), \quad x \in A_K/K.$$

特别地, 我们有

$$\sum_{\alpha\in K} \Phi(\alpha) = h_\Phi(0) = \sum_{\beta\in k} \widehat{h}_\Phi(\beta) = \sum_{\beta\in K} \widehat{\Phi}(\beta).$$

证 对 $x \in A_K/K$, 我们取 P_b 足够大, 使得当 $\beta \notin K \bigcap P_b$ 时有 $\widehat{h}_\Phi(\beta) = 0$ 以及 $h_\Phi(x + P_b^\perp) = h_\Phi(x)$. 再结合定义得

$$\begin{aligned}\sum_{\beta\in K} \widehat{h}_\Phi(\beta)\psi(-\beta x) &= \sum_{\beta\in K\cap P_b} \int_{A_K/K} h_\Phi(z)\psi(\beta z)\psi(-\beta x)\overline{\mathrm{d}z} \\ &= \int_{A_K/K} h_\Phi(z) \sum_{\beta\in K\cap P_b} \psi(\beta(z-x))\overline{\mathrm{d}z}.\end{aligned}$$

注意到

$$\sum_{\beta\in K\cap P_b}\psi(\beta(z-x))=\begin{cases}|K\bigcap P_b|, & 若 z-x\in(K\bigcap P_b)^{\perp},\\ 0, & 若 z-x\notin(K\bigcap P_b)^{\perp}.\end{cases}$$

此外，很明显 $(K\bigcap P_b)^{\perp}\supseteq K^{\perp}+P_b^{\perp}$，故

$$K\bigcap P_b\subseteq(K^{\perp}+P_b^{\perp})^{\perp}\subseteq K^{\perp\perp}\bigcap P_b^{\perp\perp}=K\bigcap P_b.$$

从而 $K\bigcap P_b=(K^{\perp}+P_b^{\perp})^{\perp}$，于是

$$(K\bigcap P_b)^{\perp}=K^{\perp}+P_b^{\perp}=K+P_{c^{-1}b}.$$

采用第四章 §4 中的记号，记 $|K\bigcap P_b|=q^{\lambda(b)}$，利用 Riemann-Roch 定理 (第四章定理 5) 有

$$\begin{aligned}\mathrm{vol}(K+P_{cb^{-1}}/K)&=\mathrm{vol}(P_{cb^{-1}}/(P_{cb^{-1}}\bigcap K))\\&=|cb^{-1}|\mathrm{vol}(P_1)/q^{\lambda(cb^{-1})}=q^{2g-2}|b^{-1}|q^{1-g}/q^{\lambda(cb^{-1})}\\&=q^{-\lambda(cb^{-1})+g-1+\deg\,\mathrm{div}\,b}=q^{-\lambda(b)},\end{aligned}$$

于是

$$\begin{aligned}\sum_{\beta\in K}\widehat{h}_{\Phi}(\beta)\psi(-\beta x)&=q^{\lambda(b)}\int_{K+P_{cb^{-1}}/K}h_{\Phi}(x)\overline{\mathrm{d}\,z}\\&=h_{\Phi}(x)q^{\lambda(b)}\mathrm{vol}(K+P_{cb^{-1}}/K)=h_{\Phi}(x).\end{aligned}$$

由此证明了反演公式.

注 我们已经看到上面的证明用到了 Riemann-Roch 定理. 事实上，如果 Φ 是平行多面体积 P_a 的特征函数，即 $\Phi=\Phi_a$，则由推论 1 知，

$$\widehat{\Phi}=|a|\,|c^{-1}|^{1/2}\Phi_{ca^{-1}}.$$

于是公式

$$\sum_{\alpha\in K}\Phi_a(\alpha)=\sum_{\beta\in K}\widehat{\Phi}_a(\beta)$$

就是 Riemann-Roch 定理. 再注意到 $K^{\perp}=K$，这一公式正好也是 Poisson 求和公式.

为了后面使用方便, 下面给出 Poisson 求和公式的一般形式.

定理 3(Poisson求和公式) 设 Φ 为 A_K 上的 Schwartz 函数, 则对任意的 $x \in I_K$ 有

$$\sum_{\alpha \in K} \Phi(x\alpha) = |x|^{-1} \sum_{\beta \in K} \widehat{\Phi}(x^{-1}\beta).$$

证 设 $g(y) = \Phi(xy)$, 则 g 也是 A_K 上的 Schwartz 函数, 其 Fourier 变换为:

$$\begin{aligned}\widehat{g}(z) &= \int_{A_K} g(y)\psi(yz)\mathrm{d}\,y = \int_{A_K} \Phi(xy)\psi(yz)\mathrm{d}\,y \\ &= \int_{A_K} \Phi(y')\psi(x^{-1}y'z)|x|^{-1}\mathrm{d}y' = |x|^{-1}\widehat{\Phi}(x^{-1}z),\end{aligned}$$

这里用到了 $\mathrm{d}y' = \mathrm{d}(xy) = |x|\mathrm{d}y$. 于是所要证的公式化为

$$\sum_{\alpha \in K} g(\alpha) = \sum_{\beta \in K} \widehat{g}(\beta).$$

而这被命题 3 所证.

§3 $Z(s, \chi, \Phi)$ 的解析开拓和函数方程

对 K 的位 v, 取 $K_v^\times$ 上的 Haar 测度 $\mathrm{d}^\times x_v$ 使得 $\mathcal{U}_v$ 的体积为 1, 由此得到 I_K 的测度 $\mathrm{d}^\times x = \prod\limits_v \mathrm{d}^\times x_v$.

引理 1 设 χ_v 是 $K_v^\times$ 的一个非分歧特征标, Φ_v 是 $\mathcal{O}_v$ 的特征函数. 当 $\mathrm{Re}\, s > 0$ 时

$$\begin{aligned}&\int_{K_v^\times} \Phi_v(x_v)\chi_v(x_v)|x_v|^s \mathrm{d}^\times x_v \\ &\qquad = (1 - \chi_v(\pi_v)\mathrm{N}v^{-s})^{-1} = L(s, \chi_v),\end{aligned}$$

其中 π_v 是 K_v 的局部单值化元素.

证 由于 Φ_v 在 $\mathcal{O}_v$ 外为 0, 故上面积分是一个在

$$\mathcal{O}_v - \{0\} = \bigcup_{n \geq 0} \mathcal{U}_v \pi_v^n$$

上的积分. 在每个集 $\mathcal{U}_v\pi_v^n$ 上, 函数 $\Phi_v(x)\chi_v(x)|x|^s$ 等于

$$\chi_v(\pi_v)^n|\pi_v|^{ns}=\chi_v(\pi_v)^n\mathrm{N}v^{-ns}$$

是个常数. 又因 $\mathcal{U}_v\pi_v^n$ 的体积为 1, 故当 $\mathrm{Re}\, s>0$ 时, 有

$$\int_{K_v^\times}\Phi_v(x_v)\chi_v(x_v)|x_v|^s\mathrm{d}^\times x_v=\sum_{n=0}^{\infty}\chi_v(\pi_v)^n\mathrm{N}v^{-ns}$$

$$=(1-\chi_v(\pi_v)\mathrm{N}v^{-s})^{-1}.$$

根据定义这恰为 $L(s,\chi_v)$, 由此引理得证.

给定一个 Schwartz 函数 Φ 和伊代尔类群 $I_K/K^\times$ 的拟特征标 χ, 定义 zeta 函数

$$Z(s,\chi,\Phi)=\int_{I_K}\Phi(x)\chi(x)|x|^s\mathrm{d}^\times\chi.$$

首先, 当 $\mathrm{Re}\, s\gg 0$ 时, 这个积分是绝对收敛的. 事实上, 存在 K 的位的有限集 S, 使得对每个不属于 S 的位 v, χ_v 是非分歧的, 且 $\Phi=\Phi_S\Phi^S$, 这里 Φ_S 是在 $\prod\limits_{v\in S}K_v^\times$ 中有紧支集的局部常值函数; $\Phi^S=\prod\limits_{v\notin S}\Phi_v$ 是所有 $\mathcal{O}_v$ $(v\notin S)$ 的特征函数的乘积. 结合引理 1, 我们就得到了

$$Z(s,\chi,\Phi)=\int_{\prod\limits_{v\in S}K_v^\times}\Phi_S(x)\left(\prod_{v\in S}\chi_v\right)(x)|x|^s\left(\prod_{v\in S}\mathrm{d}^\times x_v\right)$$

$$\times\prod_{v\notin S}\int_{K_v^\times}\Phi_v(x_v)\chi_v(x_v)|x_v|_v^s\mathrm{d}^\times x_v$$

$$=\int_{\prod_{v\in S}K_v^\times}\Phi_S(x)\left(\prod_{v\in S}\chi_v\right)(x)|x|^s\left(\prod_{v\in S}\mathrm{d}^\times x_v\right)$$

$$\times\prod_{v\notin S}L(s,\chi_v).$$

第一个积分在 $\mathrm{Re}\, s$ 充分大时是绝对收敛的, 而后一个无穷乘积恰

好等于 $L(s,\chi)\prod_{v\in S}L(s,\chi_v)^{-1}$. 注意到 $L(s,\chi)$ 在 $\mathrm{Re}\, s\gg 0$ 时绝对收敛，而对任意 $s\in S$, $L(s,\chi_v)^{-1}$ 是一个整函数，从而这一无穷乘积在 $\mathrm{Re}\, s\gg 0$ 时也绝对收敛. 由此可知 $Z(s,\chi,\Phi)$ 在 $\mathrm{Re}\, s\gg 0$ 时是有定义的. 又注意到

$$Z(s,\chi|\ |^{s_0},\Phi)=Z(s+s_0,\chi,\Phi),$$

所以我们可以假定特征标 χ 或者为平凡特征标 χ_0, 或者对任意 $t\in\mathbf{C}$, $\chi\neq|\ |^t$. 本节的目的是研究 $Z(s,\chi,\Phi)$ 的解析开拓和函数方程.

设 r 是 $\deg(I_K)$ 的正生成元，用 I_{mr} 表示次数是 mr 的伊代尔集. 于是

$$I_K=\bigcup_{m\in\mathbf{Z}}I_{mr},\quad K^\times I_{mr}=I_{mr},\quad I_{mr}=I_K^1x_0^m,$$

这里 x_0 是一个次数为 r 的伊代尔. 因此 zeta 函数 $Z(s,\chi_0,\Phi)$ 可以写为在 I_{mr} 上积分的和，而 I_{mr} 上的积分满足下面引理给出的函数方程.

引理 2

$$\int_{I_{mr}}\Phi(x)\chi(x)|x|^s\mathrm{d}^\times x+\mathcal{K}_\chi\Phi(0)q^{-mrs}$$
$$=\int_{I_{-mr}}\widehat{\Phi}(x)\chi^{-1}(x)|x|^{1-s}\mathrm{d}^\times x+\mathcal{K}_\chi\widehat{\Phi}(0)q^{mr(1-s)},$$

其中

$$\mathcal{K}_\chi=\begin{cases}\mathrm{vol}(I_K^1/K^\times) & (\text{若 }\chi=\chi_0\text{ 为平凡特征标})\\ 0, & (\text{若对任意 }t\in\mathbf{C},\ \chi\neq|\ |^t)\end{cases}$$
$$=\mathcal{K}_{\chi^{-1}}.$$

证 以 $\overline{\mathrm{d}^\times x}$ 表示由 $\mathrm{d}^\times x$ 诱导出来的 $I_K/K^\times$ 上的测度. 利用

定理 3, 我们有下面关系

$$
\begin{aligned}
&\int_{I_{mr}} \Phi(x)\chi(x)|x|^s \mathrm{d}^\times x \\
&= q^{-mrs}\int_{I_{mr}/K^\times} \chi(x) \sum_{\alpha\in K^\times} \Phi(x\alpha)\overline{\mathrm{d}^\times x} \\
&= q^{-mrs}\int_{I_{mr}/K^\times} \chi(x) \sum_{\alpha\in K} \Phi(x\alpha)\overline{\mathrm{d}^\times x} \\
&\quad - q^{-mrs}\int_{I_{mr}/K^\times} \chi(x)\Phi(0)\overline{\mathrm{d}^\times x} \\
&= q^{-mrs}\int_{I_{mr}/K^\times} \chi(x)|x|^{-1} \sum_{\alpha\in K} \widehat{\Phi}(x^{-1}\alpha)\overline{\mathrm{d}^\times x} \\
&\quad - q^{-mrs}\Phi(0)\int_{I_{mr}/K^\times} \chi(x)\overline{\mathrm{d}^\times x}.
\end{aligned} \tag{3.1}
$$

对次数为 mr 的任意伊代尔 y_0, 我们有

$$
\begin{aligned}
\int_{I_{mr}/K^\times} \chi(x)\overline{\mathrm{d}^\times x} &= \int_{I_K^1/K^\times} \chi(xy_0)\overline{\mathrm{d}^\times x} \\
&= \begin{cases} \mathrm{vol}(I_K^1/K^\times)\chi(y_0), & \text{若 } \chi \text{ 在 } I_K^1/K^\times \text{ 上平凡;} \\ 0, & \text{若 } \chi \text{ 在 } I_K^1/K^\times \text{ 上非平凡.} \end{cases}
\end{aligned}
$$

此外, 由于 χ 在 $I_K^1/K^\times$ 上平凡的充要条件是: 存在 $t\in\mathbf{C}$, 使得

$$
\chi = |\ \ |^t.
$$

所以我们可以看到, (3.1) 式的最后一项恰好为 $\mathcal{K}_\chi\Phi(0)q^{-mrs}$, 于是

$$
\begin{aligned}
&\int_{I_{mr}} \Phi(x)\chi(x)|x|^s \mathrm{d}^\times x + \mathcal{K}_\chi\Phi(0)q^{-mrs} \\
&= q^{mr(1-s)}\int_{I_{mr}/K^\times} \chi(x) \sum_{\alpha\in K^\times} \widehat{\Phi}(x^{-1}\alpha)\overline{\mathrm{d}^\times x}
\end{aligned}
$$

$$+ q^{mr(1-s)}\mathcal{K}_\chi\widehat{\Phi}(0)$$

$$= q^{mr(1-s)}\int_{I_{mr}}\chi(x)\widehat{\Phi}(x^{-1})\mathrm{d}^\times x + q^{mr(1-s)}\mathcal{K}_\chi\widehat{\Phi}(0)$$

$$= \int_{I_{-mr}}\chi^{-1}(x)\widehat{\Phi}(x)|x|^{1-s}\mathrm{d}^\times x + \mathcal{K}_\chi\widehat{\Phi}(0)q^{mr(1-s)},$$

从而引理得证.

现在我们来讨论 zeta 函数 $Z(s,\chi,\Phi)$ 的解析开拓. 利用定义

$$Z(s,\chi,\Phi) = \sum_{m\geq 0}\int_{I_{mr}}\Phi(x)\chi(x)|x|^s\mathrm{d}^\times x + \sum_{m<0}\int_{I_{mr}}\Phi(x)\chi(x)|x|^s\mathrm{d}^\times x.$$

由于 Φ 有紧支集, 故当 $m \ll 0$ 时, Φ 在 I_{mr} 上为 0. 于是第二个和式只是一个有限和, 从而是 q^{rs} 的一个多项式, 所以它对任意的 s 都是全纯的; 对于第一个和式, 利用引理 2, 当 $\mathrm{Re}\, s > 1$ 时, 有

$$\sum_{m\geq 0}\int_{I_{mr}}\Phi(x)\chi(x)|x|^s\mathrm{d}^\times x$$

$$= \sum_{m\geq 0}\int_{I_{-mr}}\widehat{\Phi}(x)\chi^{-1}(x)|x|^{1-s}\mathrm{d}^\times x$$

$$+ \mathcal{K}_\chi\widehat{\Phi}(0)\frac{1}{1-q^{r(1-s)}} - \mathcal{K}_\chi\Phi(0)\frac{1}{1-q^{-rs}}.$$

又因 $\widehat{\Phi}$ 有紧支集, 于是当 m 充分大时, $\widehat{\Phi}$ 在 I_{-mr} 上为 0, 从而上式右边给出了第一个和式的解析开拓.

总结上述讨论, 我们得到了

$$Z(s,\chi,\Phi) + \mathcal{K}_\chi\Phi(0)\frac{1}{1-q^{-rs}} - \mathcal{K}_\chi\widehat{\Phi}(0)\frac{1}{1-q^{r(1-s)}}$$

$$= \sum_{m\geq 0}\int_{I_{-mr}}\widehat{\Phi}(x)\chi^{-1}(x)|x|^{1-s}\mathrm{d}^\times x$$

$$+\sum_{m<0}\int_{I_{mr}}\Phi(x)\chi(x)|x|^{s}\mathrm{d}^{\times}x. \tag{3.2}$$

上式右边是一个 q^{rs} 和 q^{-rs} 的多项式，从而即得到 $Z(s,\chi,\Phi)$ 的解析开拓. 除了在

$$s\in 0+\frac{2\pi\mathrm{i}}{r\log q}\mathbf{Z} \quad 和 \quad s=1+\frac{2\pi\mathrm{i}}{r\log q}\mathbf{Z}$$

可能为极点之外， $Z(s,\chi,\Phi)$ 处处全纯. 特别地，当对任意 $t\in\mathbf{C}$ 都有 $\chi\neq|\ |^{t}$ 时， $\mathcal{K}_{\chi}=0$, 此时 $Z(s,\chi,\Phi)$ 可以通过 (3.2) 式解析开拓为 s 平面上的全纯函数.

接下来讨论 zeta 函数 $Z(s,\chi,\Phi)$ 的函数方程. 如同命题 2 的证明一样，我们利用 $\widehat{\widehat{\Phi}}(x)=\Phi(-x)$ 和 $\chi(-1)=1$ 将 (3.2) 式右边展开为

$$\sum_{m\leq 0}\int_{I_{mr}}\widehat{\Phi}(x)\chi^{-1}(x)|x|^{1-s}\mathrm{d}^{\times}x+\sum_{m<0}\int_{I_{mr}}\widehat{\widehat{\Phi}}(x)\chi(x)|x|^{s}\mathrm{d}^{\times}x.$$

对 I_0 上的积分应用引理 2, 上式化为

$$\sum_{m\leq 0}\int_{I_{mr}}\widehat{\widehat{\Phi}}(x)(\chi^{-1})^{-1}(x)|x|^{1-(1-s)}\mathrm{d}^{\times}x$$
$$+\sum_{m<0}\int_{I_{mr}}\widehat{\Phi}(x)\chi^{-1}(x)|x|^{1-s}\mathrm{d}^{\times}x+\mathcal{K}_{\chi}\Phi(0)-\mathcal{K}_{\chi}\widehat{\Phi}(0).$$

利用 (3.2) 式，上式正好等于

$$Z(1-s,\chi^{-1},\widehat{\Phi})+\mathcal{K}_{\chi}\widehat{\Phi}(0)\frac{1}{1-q^{-r(1-s)}}-\mathcal{K}_{\chi}\Phi(0)\frac{1}{1-q^{rs}}$$
$$+\mathcal{K}_{\chi}\Phi(0)-\mathcal{K}_{\chi}\widehat{\Phi}(0)$$
$$=Z(1-s,\chi^{-1},\widehat{\Phi})-\mathcal{K}_{\chi}\widehat{\Phi}(0)\frac{1}{1-q^{r(1-s)}}+\mathcal{K}_{\chi}\widehat{\Phi}(0)\frac{1}{1-q^{-rs}}.$$

将上式同 (3.2) 式比较即得

$$Z(s,\chi,\Phi)=Z(1-s,\chi^{-1},\widehat{\Phi}).$$

最后，我们利用 $\mathrm{vol}\left(\prod_v \mathcal{U}_v\right)=1$ 来计算 $\mathrm{vol}(I_K^1/K^\times)$. 从第三章推论 5 知

$$\mathrm{Jac}(K)\cong I_K^1/K^\times\prod_v \mathcal{U}_v.$$

又因 $K^\times\cap\prod_v \mathcal{U}_v=k^\times$, 而 $k^\times$ 的势为 $q-1$, 于是

$$\mathrm{vol}(I_K^1/K^\times)=\frac{|\mathrm{Jac}(K)|}{(q-1)}.$$

总结这一节的讨论，我们得到下面定理:

定理 4 设 r 是 $\deg(I_K)$ 的正生成元，Φ 是 A_K 上的 Schwartz 函数，χ 为 $I_K/K^\times$ 的拟特征标，且对任意 $t\in\mathbf{C}$ 都有 $\chi\neq|\ |^t$. 那么当 $\mathrm{Re}\,s$ 充分大时我们可用积分定义 zeta 函数 $Z(s,\chi,\Phi)$, 并且，它作为 q^{rs} 和 q^{-rs} 的一个多项式可以全纯开拓到 s 平面上去；对 I_K 的平凡特征标 χ_0, zeta 函数 $Z(s,\chi_0,\Phi)$ 在 $\mathrm{Re}\,s$ 充分大时亦可以用积分来定义，并且它可以亚纯开拓到 s 平面上. 精确地讲,

$$Z(s,\chi_0,\Phi)+\mathcal{K}\Phi(0)\frac{1}{1-q^{-rs}}-\mathcal{K}\widehat{\Phi}(0)\frac{1}{1-q^{r(1-s)}}$$

是 q^{rs} 和 q^{-rs} 的一个多项式，这里 $\mathcal{K}=|\mathrm{Jac}(K)|/(q-1)$. 最后，不管 χ 是什么样的特征标，zeta 函数 $Z(s,\chi,\Phi)$ 均满足函数方程

$$Z(s,\chi,\Phi)=Z(1-s,\chi^{-1},\widehat{\Phi}).$$

注 在下节我们将会看到定理中的 r 事实上为 1.

§4 K 的 zeta 函数 (定理 1 的证明)

回忆一下域 K 的 zeta 函数 $\zeta_K(s)$ 的定义:

$$\zeta_K(s)=\prod_v(1-\mathrm{N}v^{-s})^{-1}=L(s,\chi_0),$$

其中 v 过 K 的所有位. 我们已经知道，当 $\mathrm{Re}\,s\gg 0$ 时，$\zeta_K(s)$ 是

绝对收敛的. 下面命题告诉我们, 当 $\mathrm{Re}\,s>1$ 时, $\zeta_K(s)$ 已绝对收敛.

命题 4 由上面无穷乘积定义的 zeta 函数 $\zeta_K(s)$ 在 $\mathrm{Re}\,s>1$ 时绝对收敛, 并且当 $\mathrm{Re}\,s\to\infty$ 时, $\zeta_K(s)\to 1$. 此外, $\zeta_K(s)$ 在整个 s 平面上有一个亚纯延拓, $s=1$ 是它的一个残数为

$$\frac{q^{1-g}|\mathrm{Jac}K|}{(q-1)r(\log q)}$$

的单极点, 其中 r 是 $\deg(I_K)$ 的生成元.

注 同数域的情况类似, 域 K 的许多重要的算术信息都在其 zeta 函数在 $s=1$ 处的残数中反映出来, 这里, $|\mathrm{Jac}K|$ 扮演了类数的角色, $q-1$ 恰为 K 中的单位根数, 而 q^{g-1} 则类似于判别式的绝对值的平方根. 不过, 由于 K 的所有整体单位都是单位根, 所以调整子 (regulator) 在残数中没有体现.

证 为证无穷乘积的收敛性, 首先假定 $K=k(T)$ 是有理函数域. 此时, 每个不是 ∞ 的位 v 都对应了 $k[T]$ 中的一个不可约多项式 P_v, 并且有 $\deg v=\deg P_v$. 于是在 $\zeta_K(s)$ 绝对收敛时, 我们有

$$\begin{aligned}\zeta_K(s)(1-q^{-s}) &= \prod_{v\neq\infty}(1-\mathrm{N}\,v^{-s})^{-1}\\ &= \prod_{\substack{P_v\in k[T]\\ P_v:\ \text{首一, 不可约}}}(1-q^{-(\deg P_v)s})^{-1}\\ &= \sum_{\substack{m(T)\in k[T]\\ m(T):\ \text{首一}}} q^{-(\deg m(T))s}.\end{aligned}$$

对任意非负整数 n, $k[T]$ 中次数为 n 的首一多项式恰有 q^n 个, 这样

$$\zeta_K(s)(1-q^{-s})=\sum_{n\geq 0}q^nq^{-ns}=\sum_{n\geq 0}q^{n(1-s)}.$$

容易看出, 当 $\mathrm{Re}\,s>1$ 时, 上式右边的级数是绝对收敛的. 从而,

当 $\mathrm{Re}\, s > 1$ 时， $\zeta_K(s)$ 也绝对收敛．此外，上述公式也表明，当 $\mathrm{Re}\, s \to \infty$ 时， $\zeta_K(s) \to 1$.

下面假定 K 是有理函数域 $F = k(T)$ 的 n 次可分扩张．则

$$\zeta_K(s) = \prod_{v:\, F\text{的位}} \prod_{\substack{w:\, K\text{的位} \\ w|v}} (1 - \mathrm{N}\, w^{-s})^{-1}.$$

设 S 是由有限多个 F 的位组成的集合，并且任意 S 外 F 的位对于扩张 K/F 都是非分歧的．任取一个 F 的不在 S 中的位 v, 由第三章定理 3 和定理 4 可知

$$n = \sum_{w|v} [K_w : F_v] = \sum_{w|v} [k_w : k_v],$$

其中 k_w 和 k_v 分别为 K_w 和 F_v 的剩余类域．设 w 是 K 的一个整除 v 的位，假定 $[K_w : F_v] = m$, 则 $\mathrm{N}\, w = (\mathrm{N}\, v)^m$．注意到，当 $\sigma = \mathrm{Re}\, s > 1$ 时，有

$$(1 - \mathrm{N}\, w^{-\sigma})^{-1} \le (1 - \mathrm{N}\, v^{-\sigma})^{-m},$$

即

$$(1 - \mathrm{N}\, v^{-\sigma})^m \le 1 - (\mathrm{N}\, v^{-\sigma})^m .$$

这是因为通过两边同除以 $1 - \mathrm{N}\, v^{-\sigma}$, 可以看到，所需不等式等价于

$$(1 - \mathrm{N}\, v^{-\sigma})^{m-1} \le 1 + \mathrm{N}\, v^{-\sigma} + \mathrm{N}\, v^{-2\sigma} + \cdots + \mathrm{N}\, v^{-(m-1)\sigma},$$

而后一个不等式是显然的．于是，当 $\sigma = \mathrm{Re}\, s > 1$ 时，我们有

$$\begin{aligned} \zeta_K(\sigma) \prod_{v\in S} \prod_{w|v} (1 - \mathrm{N}\, w^{-\sigma}) &= \prod_{v\notin S} \prod_{w|v} (1 - \mathrm{N}\, w^{-\sigma})^{-1} \\ &\le \prod_{v\notin S} (1 - \mathrm{N}\, v^{-\sigma})^{-n} = \zeta_F(\sigma)^n \prod_{v\in S} (1 - \mathrm{N}\, v^{-\sigma})^n, \end{aligned}$$

其中 v 过 F 的位集， w 过 K 的位集．由此，结合前面对有理函数域的讨论，我们可以断言， ζ_K 在 $\mathrm{Re}\, s > 1$ 时绝对收敛，且当 $\mathrm{Re}\, s \to \infty$ 时， $\zeta_K(s) \to 1$.

取 $\Phi = \Phi_1$ 是平行多面体 $P_1 = \prod_w O_w$ 的特征函数，从上一节的讨论可以看到 $Z(s, \chi_0, \Phi_1) = \zeta_K(s)$. 于是由定理 4 我们就可肯定 ζ_K 可以亚纯延拓到整个 s 平面上. 此外，从定理 4 也可看到 $\zeta_K(s)$ 在 $s = 1$ 处有一个单极点，其残数恰为 $\mathcal{K}\widehat{\Phi}_1(0)\dfrac{1}{1-q^{r(1-s)}}$ 在 $s=1$ 处的残数，我们已知

$$\mathcal{K} = |\mathrm{Jac}K|/(q-1)$$

和

$$\widehat{\Phi}_1(0) = |c^{-1}|^{1/2}\Phi_1(0) = q^{1-g},$$

此外，$\dfrac{1}{1-q^{r(1-s)}}$ 在 $s=1$ 处残数为 $\dfrac{1}{r\log q}$, 由此就得到了

$$\mathrm{Res}_{s=1}\zeta_K(s) = \frac{q^{1-g}|\mathrm{Jac}K|}{(q-1)r(\log q)}.$$

进而命题得证.

现在我们可以证明 $\deg(I_K) = \mathbf{Z}$. 事实上，我们将证明下面这个更强的结果：

定理 5 设 S 是由有限多个 K 的位组成的集合，则存在 K 的一个次数为 1 的除子 $\sum_v n_v v$, 使得当 $v \in S$ 时，$n_v = 0$. 特别地，$\deg(I_K) = \mathbf{Z}$.

证 设 A 表示集合

$$\{x = (x_v) \in I_K : 当 v \in S 时, x_v 为单位\}.$$

易证 A 是 I_K 的一个子群，故 $\deg(A)$ 是 $\mathbf{Z}$ 中的一个无限循环子群. 设 $\deg(A)$ 生成元为 l, 我们的任务是证明 $l = 1$.

以 L 来表示域 K 与 k_l 的合成，则 L 是 K 的一个有限可分扩张，记 $n = [L : K]$. 又取一个由有限多个 K 的位组成的集合 S', 它包含 S, 并且对任意的 $v \notin S'$, 扩张 L/K 关于位 v 是非分歧的.

设 v 是 K 的一个不在 S' 中的位，则

$$\bigoplus_{\substack{w:L \text{ 的位} \\ w|v}} L_w = K_v \bigotimes_K L$$

是通过给 K_v 添加 q^l-1 次单位根而得到的代数. 特别地, 每个 L_w 均可由 K_v 添加一个 q^l-1 次单位根后得到. 由假设知, 存在自然数 m, 使得 $\deg v = ml$. 于是 K_v 的剩余类域是 k_{ml}, 这就说明 K_v 包含了所有 q^l-1 次单位根, 从而对所有 $w|v$ 均有 $L_w \cong K_v$. 这样, 对任意的不在 S' 中的 K 的位 v, 存在 n 个 L 的可整除 v 的位 w, 使得每个 L_w 同构于 K_v. 于是

$$\begin{aligned}
\zeta_L(s) &= \prod_{\substack{v\notin S' \\ v:K \text{ 的位}}} \prod_{w|v}(1-\mathrm{N}\,w^{-s})^{-1} \prod_{v\in S'}\prod_{w|v}(1-\mathrm{N}\,w^{-s})^{-1} \\
&= \prod_{v\notin S'}(1-\mathrm{N}\,v^{-s})^{-n} \prod_{v\in S'}\prod_{w|v}(1-\mathrm{N}\,w^{-s})^{-1} \\
&= \zeta_K(s)^n \prod_{v\in S'}\Big((1-\mathrm{N}\,v^{-s})^{n}\prod_{w|v}(1-\mathrm{N}\,w^{-s})^{-1}\Big).
\end{aligned}$$

对每个 $v \in S'$, $(1-\mathrm{N}\,v^{-s})^n \prod_{w|v}(1-\mathrm{N}\,w^{-s})^{-1}$ 在 $s=1$ 处全纯且非零. 又从命题 4 知, $\zeta_K(s)$ 在 $s=1$ 处有个单极点, 从而 $\zeta_L(s)$ 在 $s=1$ 处有个 n 阶极点. 然而, 命题 4 同样指出 $\zeta_L(s)$ 在 $s=1$ 处只有单极点, 这就导出 $n=1$, 即 $L=K$. 从而 K 包含 k_l. 又因 k 是 K 的常数域, 所以 $k_l = k$, 即 $l=1$.

从定理 5 就可看出, 定理 4 和命题 4 中的 r 均等于 1.

注 设 K 是个整体域, L 为 K 的 n 次可分扩张. 对 K 的一个位 v, 如果恰有 n 个 L 的位整除 v, 则我们称 v 在 L 中**完全分裂**. 上面的讨论表明, 对函数域情形而言, 如果几乎所有的 K 的位在 L 中完全分裂, 则 $L=K$. 更精确一些, Čebotarev 密度定理告诉我们, 在 L 中完全分裂的 K 的位的密度是 $1/n$. 这些结论对数域的情况同样也是正确的.

从定理 4 可知,

$$\zeta_K(s)+\frac{\mathcal{K}}{1-q^{-s}}-\frac{\mathcal{K}q^{1-g}}{1-q^{1-s}}$$

是 q^s 和 q^{-s} 的多项式, 而命题 4 告诉我们, 当 $\mathrm{Re}\,s\to\infty$ 时, $\zeta_K(s)\to 1$. 结合起来可以断定

$$\zeta_K(s)+\frac{\mathcal{K}}{1-q^{-s}}-\frac{\mathcal{K}q^{1-g}}{1-q^{1-s}}$$

是 q^{-s} 的多项式. 命 $U=q^{-s}$. 我们已知, $\zeta_K(s)$ 可以写成 $Z_C(q^{-s})$, 这里 $Z_C(q^{-s})$ 是一条非奇异射影曲线 C 的 zeta 函数, 从而有

$$Z_C(U)=\frac{P_1(U)}{(1-U)(1-qU)},$$

其中 $P_1(U)$ 是一个 U 的多项式. 故

$$P_1(0)=Z_C(0)=\lim_{\mathrm{Re}\,s\to\infty}\zeta_K(s)=1.$$

此外

$$\begin{aligned}\frac{P_1(1)}{q-1}&=\mathrm{Re}\,s_{U=1}Z_C(U)\\&=\mathrm{Re}\,s_{U=1}\left(-\frac{\mathcal{K}}{1-U}\right)=\mathcal{K}=\frac{|\mathrm{Jac}K|}{q-1}.\end{aligned}$$

于是 $P_1(1)=|\mathrm{Jac}K|$. 借助于函数方程

$$Z(s,\chi_0,\Phi_1)=Z(1-s,\chi_0,\widehat{\Phi}_1),$$

$$\widehat{\Phi}_1(x)=|c^{-1}|^{1/2}\Phi_1(c^{-1}x)\quad(\text{见}\,\S2\,\text{中的推论}\,1)$$

和

$$\begin{aligned}Z(1-s,\chi_0,\widehat{\Phi}_1)&=\int_{I_K}|c^{-1}|^{1/2}\Phi_1(c^{-1}x)|x|^{1-s}\mathrm{d}^\times x\\&=|c|^{\frac{1}{2}-s}\int_{I_K}\Phi_1(x)^{1-s}\mathrm{d}^\times x\\&=q^{(\frac{1}{2}-s)(2g-2)}L(1-s,\chi_0)=q^{(\frac{1}{2}-s)(2g-2)}\zeta_K(1-s),\end{aligned}$$

我们有

$$\zeta_K(s) = q^{(\frac{1}{2}-s)(2g-2)}\zeta_K(1-s).$$

从而导出 $P_1(U)$ 应满足函数方程

$$P_1(U) = (q^{1/2}U)^{2g} P_1\left(\frac{1}{qU}\right). \tag{4.1}$$

又因 $P_1(U)$ 是 U 的多项式, 故上式意味着 $\deg P_1 \leq 2g$. 若 $\deg P_1 < 2g$, 则在 $U=0$ 时, (4.1) 式右边应等于 0, 这与其左边 $P_1(0)=1$ 矛盾, 故 $\deg P_1 = 2g$. 最后, 由

$$P_1(U) = Z_C(U)(1-U)(1-qU)$$

以及

$$Z_C(U) = \prod_v (1-U^{\deg v})^{-1}$$

是一个整系数的无穷乘积, 可以断定 $P_1(U)$ 是一个整系数多项式. 由此我们完成了定理 1 的证明.

§5 具有非平凡特征标 χ 的 L-函数 $L(s,\chi)$ (定理 2 之证明)

在这一节中, 我们假定 χ 是伊代尔类群 $I_K/K^\times$ 的一个特征标, 且对任意复数 $t \in \mathbf{C}$, 均有 $\chi \neq |\ |^t$. 用

$$\mathfrak{f}(\chi) = \sum_v n_v v$$

表示 χ 的前导子, S 表示 $\mathfrak{f}(\chi)$ 的支集. 则

$$L(s,\chi) = \prod_{v\notin S}(1-\chi_v(\pi_v)\mathrm{N}v^{-s})^{-1}.$$

利用命题 4 的证明, 我们可以断言 $L(s,\chi)$ 在 $\mathrm{Re}\ s>1$ 时绝对收敛, 且当 $\mathrm{Re}\ s\to\infty$ 时 $L(s,\chi)\to 1$. 设 a 是一个满足 $\mathrm{div}\, a = \mathfrak{f}(\chi)$ 的伊代尔, Φ 为 $(1+P_a)$ 的特征函数. 于是在每个不属于 S 的位

v 处，由于 χ_v 是非分歧的，故 Φ 在 K_v 上的限制是 $\mathcal{O}_v$ 的特征函数；在位 $v\in S$ 处，Φ 在 K_v 上的限制是 $1+\mathfrak{p}_v^{n_v}$ 的特征函数，而在这上面 χ_v 是平凡的. 从而我们有

$$Z(s,\chi,\Phi)=\prod_{v\notin S}L(s,\chi_v)\prod_{v\in S}\int_{1+\mathfrak{p}_v^{n_v}}\chi_v(x_v)|x_v|^s\mathrm{d}^\times x_v$$

$$=L(s,\chi)\prod_{v\in S}\mathrm{vol}(1+\mathfrak{p}_v^{n_v}).$$

从定理 4 可知，$L(s,\chi)$ 作为 q^s 和 q^{-s} 的多项式可以全纯开拓至整个 s 平面. 结合当 $\mathrm{Re}\,s\to\infty$ 时，$L(s,\chi)\to 1$, 我们可以断定，存在一个 U 的多项式 $P(U,\chi)$, 使得

$$L(s,\chi)=P(q^{-s},\chi).$$

为导出 $L(s,\chi)$ 的函数方程，下面我们来研究 $Z(1-s,\chi^{-1},\widehat{\Phi})$. 由推论 2 知

$$\widehat{\Phi}=\psi\widehat{\Phi}_a=|a||c^{-1}|^{1/2}\psi\Phi_{ca^{-1}}.$$

于是，当 $\mathrm{Re}\,s$ 充分大时，

$$Z(1-s,\chi^{-1},\widehat{\Phi})=|a|\,|c^{-1}|^{1/2}\int_{I_K}\psi(x)\Phi_{ca^{-1}}(x)\chi^{-1}(x)|x|^{1-s}\mathrm{d}^\times x$$

$$=|a|\,|c^{-1}|^{1/2}|ca^{-1}|^{1-s}$$

$$\times\int_{I_K}\psi(ca^{-1}x)\Phi_1(x)\chi^{-1}(ca^{-1}x)|x|^{1-s}\mathrm{d}^\times x.$$

当位 v 不在 S 中时，Φ_1 在 K_v 上的限制是 $\mathcal{O}_v$ 的特征函数，此时 $\psi_v(c_va_v^{-1}x_v)$ 是平凡的且 χ_v 非分歧. 从而

$$Z(1-s,\chi^{-1},\widehat{\Phi})$$

$$=|a|^s|c|^{\frac{1}{2}-s}\chi^{-1}(ca^{-1})L(1-s,\chi^{-1})$$

$$\times\prod_{v\in S}\int_{\mathcal{O}_v-\{0\}}\psi_v(c_va_v^{-1}x_v)\chi_v^{-1}(x_v)|x_v|^{1-s}\mathrm{d}^\times x_v.$$

记 $\mathcal{O}_v - \{0\} = \bigcup_{n=0}^{\infty} \mathcal{U}_v \pi_v^n$. 当 $n \geq 1$ 时,

$$\int_{\mathcal{U}_v \pi_v^n} \psi_v(c_v a_v^{-1} x_v) \chi_v^{-1}(x_v) |x_v|^{1-s} \mathrm{d}^\times x_v$$

$$= \begin{cases} \dfrac{1}{(Nv)^{n(1-s)}} \displaystyle\sum_{y_v \in \mathcal{U}_v/(1+\mathfrak{p}_v^{n_v - n})} \psi_v(c_v a_v^{-1} \pi_v^n y_v) \chi_v^{-1}(\pi_v^n y_v) \\ \qquad \times \displaystyle\int_{1+\mathfrak{p}_v^{n_v-n}} \chi_v^{-1}(x_v) \mathrm{d}^\times x_v, & \text{若} n < n_v, \\ \dfrac{1}{(Nv)^{n(1-s)}} \displaystyle\int_{\mathcal{U}_v} \chi_v^{-1}(x_v \pi_v^n) \mathrm{d}^\times x_v, & \text{若} n \geq n_v. \end{cases}$$

又因 χ_v 在 $1 + \mathfrak{p}_v^{n_v - 1}$ 上非平凡, 故上式等于 0. 从而当 $v \in S$ 时, 过 $\mathcal{O}_v - \{0\}$ 的积分是一个非零常数 (可以表成一个 Gauss 和). 于是, 存在常数 β, 使得

$$Z(1-s, \chi^{-1}, \widehat{\Phi}) = \beta q^{(\frac{1}{2}-s)(2g-2+\deg \mathfrak{f}(\chi))} L(1-s, \chi^{-1}).$$

从而由函数方程 $Z(s, \chi, \Phi) = Z(1-s, \chi^{-1}, \widehat{\Phi})$ 导出了 $L(s, \chi)$ 的函数方程

$$L(s, \chi) = c(\chi) q^{(\frac{1}{2}-s)(2g-2+\deg \mathfrak{f}(\chi))} L(1-s, \chi^{-1}),$$

即

$$P(U, \chi) = c(\chi)(q^{\frac{1}{2}} U)^{(2g-2+\deg \mathfrak{f}(\chi))} P\left(\frac{1}{qU}, \chi^{-1}\right).$$

其中 $c(\chi)$ 是一个非零常数. 又因 $P(U, \chi)$ 是 U 的多项式, 从而 $P(U, \chi^{-1})$ 是一个次数不超过 $2g - 2 + \deg \mathfrak{f}(\chi)$ 的多项式. 再结合 $P(0, \chi) = 1$, 我们可以判断出 $P(U, \chi^{-1})$ 的次数恰为

$$2g - 2 + \deg \mathfrak{f}(\chi),$$

进而 $P(U, \chi)$ 也是一个 $2g - 2 + \deg \mathfrak{f}(\chi)$ 次多项式. 由此完成了定理 2 之证明.

注 利用上面的讨论，非零常数 $c(\chi)$ 事实上可以表为

$$c(\chi) = q^{(2-2g-\deg \mathfrak{f}(x))/2} \prod_{v\in S} \prod_{x_v\in \mathcal{U}_v/(1+\mathfrak{p}_v^{n_v})} [\psi_v(c_v a_v^{-1} x_v) \times \chi_v^{-1}(c_v a_v^{-1} x_v)] \prod_{v\notin S} \chi_v^{-1}(c_v).$$

参 考 文 献

[1] L. J. Goldstein, *Analytic Number Theory*, Prentice-Hall Inc. New Jersy, 1971.

[2] S. Lang, *Algebraic Number Theory*, GTM 110, Springer-Verlag, New York, 1986.

[3] J. Tate, *Fourier Analysis in Number Fields and Hecke's Zeta-Functions*, Thesis, Princeton University, 1950, Published in *Algebraic Number Theory*, J. W. S. Cassels and A. Frohlich edited, Thompson, Washington D. C. 1967, republished by Academic Press, London, 1989.

[4] A. Weil, *Basic Number Theory*, Springer-Verlag, Berlin-Heidelberg-New York, 1973.

第六章　特征和估计与伊代尔类特征标

在这一章中，我们着重研究一些特征和的估计，这些特征和的估计在数论的许多研究中都扮演了重要角色.

§1　L-函数的根

在第五章中我们研究了结合函数域的伊代尔类群之特征标的 L-函数的解析性质，在这一节中，我们将研究这些 L-函数根的性质，这将是后面特征和估计研究的基础. 在这一章中我们将假定读者熟悉类域论的一些结论，不了解类域论的读者可以参阅参考文献 [2, 6, 11].

和第五章一样，如无特殊说明，k 总表示一个有 q 个元素的有限域，K 是常数域为 k、亏格为 g_K 的单变量函数域. 设 $\overline{K}$ 是 K 的一个可分闭包. 对 Galois 群 $\mathrm{Gal}(\overline{K}/K)$ 赋以 Krull 拓扑，即取 $\{\mathrm{Gal}(\overline{K}/F) : F$ 为 $\overline{K}$ 中 K 的有限 Galois 扩张 $\}$ 作为 $\mathrm{Gal}(\overline{K}/K)$ 中单位映射的一个基本领域系. 在 Krull 拓扑下，Galois 群 $\mathrm{Gal}(\overline{K}/K)$ 成为一个全不连通的拓扑群. 结合 $\mathrm{Gal}(\overline{K}/K)$ 的每一个有限维表示 ρ, Artin 定义了一个 L-函数 $L(s,\rho)$. 当 ρ 是 $\mathrm{Gal}(\overline{K}/K)$ 的平凡表示时，L-函数 $L(s,\rho)$ 就是 K 的 zeta 函数 $\zeta_K(s)$. 对 $\mathrm{Gal}(\overline{K}/K)$ 的一个一维表示 (即特征标) ρ, 存在 K 在 $\overline{K}$ 中的一个有限 Abel 扩张 F, 使得 ρ 可以视为

$$\mathrm{Gal}(F/K) \cong \mathrm{Gal}(\overline{K}/K)/\mathrm{Gal}(\overline{K}/F)$$

的特征标. 利用整体类域论可知，$I_K/K^\times \mathrm{N}_{F/K}(I_F)$ 与 $\mathrm{Gal}(F/K)$ 同构，从而存在 $I_K/K^\times \mathrm{N}_{F/K}(I_F)$ 的一个伊代尔类特征标 χ, 使得 $L(s,\chi) = L(s,\rho)$. 反过来，给出一个 $I_K/K^\times$ 的有限阶特征标 χ, 则

存在 K 的一个有限 Abel 扩张 F, 使得 $I_K/\ker\chi$ 同构于 $\mathrm{Gal}(F/K)$. 进而可找到 $\mathrm{Gal}(F/K)$ 的一个一维表示 ρ, 使得

$$L(s,\chi)=L(s,\rho).$$

因此, 在 $I_K/K^\times$ 的有限阶特征标与 $\mathrm{Gal}(\overline{K}/K)$ (或 $\mathrm{Gal}(K^{ab}/K)$) 的特征标之间有一个一一对应, 其对应的特征标结合同样的 L-函数. 于是对 $I_K/K^\times$ 的有限阶特征标对应的 L-函数的根的研究就化为研究结合 $\mathrm{Gal}(\overline{K}/K)$ 的特征标的 L-函数的根. 从第五章中的命题 1 知, $I_K/K^\times$ 的任意拟特征标 η 均可写成一个有限阶伊代尔特征标 χ 和某个 $|\ |^{s_0}(s_0\in\mathbf{C})$ 的乘积. 于是

$$L(s,\eta)=L(s,\chi|\ |^{s_0})=L(s+s_0,\chi).$$

从而对 $L(s,\eta)$ 的根的研究可以由对 $L(s,\chi)$ 的研究中得到.

设 F 是 K 的有限 Abel 扩张, 1_F 是

$$\mathrm{Gal}(\overline{K}/F)=\mathrm{Gal}(\overline{F}/F)$$

的平凡表示, 则诱导表示

$$\rho=\mathrm{Ind}\,_{\mathrm{Gal}(\overline{K}/F)}^{\mathrm{Gal}(\overline{K}/K)}1_F=\mathrm{Ind}\,_{\{\mathrm{id}\}}^{\mathrm{Gal}(F/K)}1$$

是 $\mathrm{Gal}(F/K)$ 的一个次数为 $[F:K]$ 的正则表示, 并且它可以分解为 $\mathrm{Gal}(F/K)$ 的次数为 1 的表示 ρ_i 的直和, 而且每个 ρ_i 只出现一次, 即 $\rho=\bigoplus\limits_i\rho_i$. 于是从 Artin L-函数的性质可得

$$\begin{aligned}\zeta_F(s)=L(s,1_F)=L(s,\rho)&=\prod_i L(s,\rho_i)\\&=\zeta_K(s)\prod_{\rho_i\neq 1_K}L(s,\rho_i).\end{aligned}$$

注意到 F 的常数域是 k 的一个有限扩张, 我们以 k_n 表示, 它的势为 q^n. 由第五章之定理 1 知

$$\zeta_F(s)=\frac{P_F(q^{-ns})}{(1-q^{-ns})(1-q^{n(1-s)})},$$

$$\zeta_K(s)=\frac{P_K(q^{-s})}{(1-q^{-s})(1-q^{1-s})},$$

其中 $P_F(u)$ 和 $P_K(u)$ 分别为次数 $2g_F$ 和 $2g_K$ 的多项式. 进一步, 以 χ_i 表示使得 $L(s,\chi_i)=L(s,\rho_i)$ 的 $I_K/K^\times$ 的特征标. 从第五章中的定理 1 和定理 2 知, 若对任意的 $s_0\in\mathbf{C}$, 均有 $\chi_i\neq|\ |^{s_0}$, 则

$$L(s,\chi_i)=P(q^{-s},\chi_i),$$

其中 $P(u,\chi_i)$ 是 u 的次数为 $2g_K-2+\deg\mathfrak{f}(\chi_i)$ 的多项式, 这里同以前一样, $\mathfrak{f}(\chi)$ 表示特征标 χ 的前导子. 若存在 $s_0\in\mathbf{C}$, 使得 $\chi_i=|\ |^{s_0}$, 则 $L(s,\chi_i)=\zeta_K(s+s_0)$. 此时若以 $P(q^{-s},\chi_i)$ 表示 $L(s,\chi_i)$ 的分子, 则 $P(u,\chi_i)$ 是一个次数为 $2g_K$ 的多项式. 我们断言有下面结果.

定理 1 记号同前, 则 $P_F(u^n)=\prod\limits_{\chi_i}P(u,\chi_i)$, 其中 χ_i 跑遍 $I_K/K^\times$ 的与 $\rho_i\in\widehat{\mathrm{Gal}(F/K)}$ 对应的所有伊代尔类特征标, 即所有 $I_K/K^\times\mathrm{N}_{F/K}(I_F)$ 的特征标.

从关系式 $\zeta_F(s)=\prod\limits_{\chi_i}L(s,\chi_i)$ 对 L-函数的研究看出, 问题的关键是研究 $\chi_i=|\ |^{s_0}$ 这种情况. 此外, 我们还提醒一下读者, 由第五章的定理 5 知, I_K 中存在一个次数为 1 的伊代尔. 在证明定理 1 之前, 我们先证明下述命题.

命题 1 设 k_m 是 k 在 $\overline{K}$ 中的 m 次扩张, E 是 K 与 k_m 的合成. 则 E 是 K 的一个 m 次非分歧 Abel 扩张. 对 K 的任意位 v 和 E 的任意可整除 v 的位 w, 有 $\deg w=(\deg v)/d_v$ 及 $[E_w:K_v]=m/d_v$, 其中 $d_v=[k_m\bigcap K_v:k]$. 此外, 若 t 是 I_K 的一个次数为 1 的伊代尔, 则 $\mathrm{N}_{E/K}(I_E)K^\times=I_k^1\langle t\rangle^m$.

这里从 I_E 到 I_K 的范数映射是局部范数的积. 即对

$$x=(x_w)\in I_E,\quad \mathrm{N}_{E/K}(x)=\left(\prod_{w|v}\mathrm{N}_{E_w/K_v}(x_w)\right)\in I_K.$$

证 设 ζ 是 k_m 中一个 q^m-1 次单位根, 又设 $f(x)$ 是 ζ 在

k 上的极小多项式，则 $\deg f = m$. 显然，$E = K(\zeta)$ 是 K 的 Abel 扩张. 又因 K 的常数域是 k, 故 $[E : K] = \deg f = m$. 设 v 是 K 的一个位. 将 $f(x)$ 在 K_v 上分解为不可约多项式之积

$$f(x) = f_1(x) \cdots f_r(x),$$

则由 Hensel 引理知，每个 $\overline{f_i(x)}$ 在 K_v 的剩余类域 κ_v 上不可约，且 $\deg \overline{f_i} = \deg f_i$. 对任意可整除 v 的 E 的位 w, 存在 i, 使得 $E_w \cong K_v[x]/(f_i(x))$. 从而

$$[E_w : K_v] = \deg f_i = [\kappa_w : \kappa_v],$$

其中 κ_w 表示 E_w 的剩余类域. 换句话说，E_w 在 K_v 上非分歧. 又设 $d_v = [\kappa_v \bigcap k_m : k]$. 由于 $\kappa_w = \kappa_v k_m$, 即 κ_v 与 k_m 的合成，我们有

$$[E_w : K_v] = [\kappa_w : \kappa_v] = [k_m : k_m \bigcap \kappa_v] = m/d_v,$$

以及

$$\deg w = [\kappa_w : k_m] = [\kappa_v : \kappa_v \bigcap k_m] = (\deg v)/d_v (\text{见图}2).$$

此外，由于 E_w 在 K_v 上非分歧，故 K_v 的一个局部单值化元素 π_v 同时也是 E_w 的局部单值化元素，不过，有时为表述明确起见，仍用不同的记号表示.

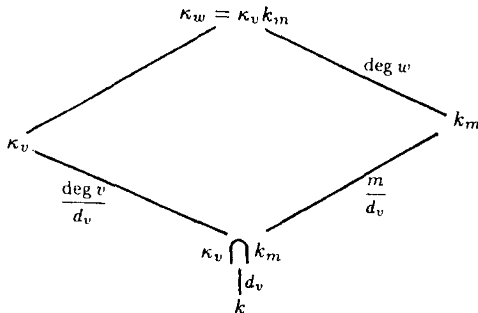


图 2

取

$$y = \prod_{w:E\text{的位}} \pi_v^{n_w}$$

是一个 E 的一个次数为 1 的 E 的伊代尔. 因此, 对所有的 w, $n_w \in Z$, 并且对几乎的所有的 w, $n_w = 0$, 以及

$$1 = \sum_w n_w \deg \omega = \sum_{v:K\text{的位}} \left(\sum_{w|v} n_w \right) \frac{\deg v}{d_v}.$$

从而

$$\begin{aligned} \mathrm{N}_{E/K}(y) &= \prod_{v:K\text{的位}} \prod_{w|v} \mathrm{N}_{E_w/K_v}(\pi_w)^{n_w} \\ &= \prod_v \prod_{w|v} \pi_v^{n_w[E_w:E_v]} \\ &= \prod_v \pi_v^{\left(\sum\limits_{w|v} n_w\right) m/d_v} \in I_K, \end{aligned}$$

以及

$$\deg \mathrm{N}_{E/K}(y) = \sum_v \left(\sum_{w|v} n_w \right) \frac{m}{d_v} \deg v = m.$$

显然, $\mathrm{N}_{E/K}(I_E^1) \subset I_K^1$. 此外, 对 I_K 中任意次数为 1 的伊代尔 t, 有 $I_K = I_K^1\langle t\rangle$; 并且 $I_K^1 t^m$ 是 I_K 中所有次数为 m 的伊代尔组成的集合, 特别地, 它包含了 $\mathrm{N}_{E/K}(y)$. 这就表明

$$\mathrm{N}_{E/K}(I_E)K^\times \subset I_K^1\langle t\rangle^m.$$

由

$$I_K/\mathrm{N}_{E/K}(I_E)K^\times \cong \mathrm{Gal}(E/K)$$

可知, $\mathrm{N}_{E/K}(I_E)K^\times$ 是 I_K 的一个指数 m 的开子群. 此外, 再注意到 $I_K^1\langle t\rangle^m$ 也是 I_K 的指数 m 的子群, 于是结合前面讨论可得

$$\mathrm{N}_{E/K}(I_E)K^\times = I_K^1\langle t\rangle^m.$$

推论 1 对 K 的任意位 v 和 E 的任意整除 v 的位 ω, 有

$$\mathrm{N}_{E_w/K_v}(\mathcal{U}_w) = \mathcal{U}_v.$$

定理 1 的证明 我们已经知道, 对应于表示 ρ_i 的特征标 χ_i 是 $I_K/K^\times \mathrm{N}_{F/K}(I_F)$ 的特征标, 即那些核包含了 $K^\times \mathrm{N}_{F/K}(I_F)$ 的 I_K 的特征标. 域 F 包含子域 $E = K \cdot k_n$. 从前面的命题 1 可知,

$$I_K^1 \langle t \rangle^n = \mathrm{N}_{E/K}(I_E)K^\times \supset \mathrm{N}_{F/K}(I_F)K^\times.$$

从而 $I_K/I_K^1\langle t\rangle^n$ 的特征标是那些具有形式 $\eta = |\ |^{s_0}$, $s_0 \in \mathbf{C}$, 且 $\eta^n = 1$ 的特征标 η. 因此这些 η 是特征标 χ 中的一部分, 并且存在一个 n 次单位根 $\zeta = \eta(t)$, 使得

$$L(s,\eta) = \frac{P_K(\zeta q^{-s})}{(1-\zeta q^{-s})(1-\zeta q^{1-s})}.$$

全体这样的 $L(s,\eta)$ 的乘积, 其分母是 $(1-q^{-ns})(1-q^{n(1-s)})$, 并且 $P(u,\eta) = P(\zeta u, \chi_0)$, 其中 χ_0 是 I_K 的平凡特征标. 设 H 是由具有形式 $|\ |^{s_0}$, $s_0 \in \mathbf{C}$ 的特征标 χ_i 生成的 $\widehat{I_K/K^\times \mathrm{N}_{F/K}(I_F)}$ 的子群. 由于这样的特征标 χ_i 在 I_K^1 上平凡, 所以 H 是一个 m 阶循环群, 恰好是 $I_K/I_K^1\langle t\rangle^m$ 的对偶群. 我们已知 $n|m$, 进而对域 $E' = Kk_m$ 应用命题 1 可得

$$I_K^1\langle t\rangle^m = K^\times \mathrm{N}_{E'/K}(I_E').$$

利用类域论知, $K^\times \mathrm{N}_{E'/K}(I_E')$ 包含 $K^\times \mathrm{N}_{F/K}(I_F)$, E' 为 F 的子域. 这就表明, k_m 含在 F 的常数域 k_n 中, 从而 $k_m = k_n$, 即 $m = n$. 我们已经证明了恰有 n 个可以对应 ρ_i 的特征标 χ_i 具有 $|\ |^{s_0}(s_0 \in \mathbf{C})$ 的形式, 于是其他特征标所结合的 L-函数就只能是 q^{-s} 的多项式. 综上所述, 定理得证.

第四章的定理 8 告诉我们关于域 F 的 Riemann 猜测成立, 即存在 ω_i, 且 $|\omega_i| = q^{n/2}$, 使得

$$P_F(U) = \prod_{i=1}^{2g_F}(1-\omega_i U).$$

于是存在 β_j, 且 $|\beta_j| = q^{1/2}$, 使得

$$P_F(u^n) = \prod_{i=1}^{2g_F}(1-\omega_i u^n) = \prod_{j=1}^{2ng_F}(1-\beta_j u).$$

结合定理 1 就可推出多项式 $P(u,\chi_i)$ 所有根的绝对值均为 $q^{-1/2}$. 利用本节开始时的分析, 总结上述讨论, 我们就证明了下面结果.

定理 2 设 χ 是 I_K 的一个有限阶伊代尔类特征标. 用 $P(q^{-s},\chi)$ 表示 $L(s,\chi)$ 的分子, 则 $P(u,\chi)$ 根的绝对值均为 $q^{-1/2}$.

推论 2 设 χ 是 I_K 的一个有限阶伊代尔类特征标, 且对任意 $s_0 \in \mathbf{C}$ 均有 $\chi \neq |\ |^{s_0}$. 设 $\mathfrak{f}(\chi)$ 为 χ 之前导子, 则

$$L(s,\chi) = P(q^{-s},\chi),$$

其中 $P(u,\chi) = 1 + a_1 u + a_2 u^2 + \cdots + a_r u^r$ 是一个次数为

$$r = 2g_K - 2 + \deg \mathfrak{f}(\chi)$$

的多项式, 并且

$$|a_1| \le (2g_K - 2 + \deg \mathfrak{f}(\chi))\sqrt{q}, \qquad |a_r| = q^{r/2}.$$

回忆一下 L-函数 $L(s,\chi)$ 的定义

$$L(s,\chi) = \prod_v L(s,\chi_v) = \prod_{\substack{v \\ \chi_v \text{ 非分歧}}} (1-\chi_v(\pi_v)(\mathrm{N}v)^{-s})^{-1},$$

其中 $\mathrm{N}v = q^{\deg v}$. 于是

$$a_1 = \sum_{\substack{\deg v = 1 \\ \chi_v \text{ 非分歧}}} \chi_v(\pi_v).$$

进而由推论 2 得

推论 3 采用与推论 2 同样的记号, 则

$$\left|\sum_{\substack{\deg v = 1 \\ \chi_v \text{ 非分歧}}} \chi_v(\pi_v)\right| \le (2g_K - 2 + \deg \mathfrak{f}(\chi))\sqrt{q}.$$

上述不等式是我们后面研究特征和估计的基础. 简单地讲, 给出一个特征和, 我们将试图构造一个有限阶伊代尔类特征标 χ, 使得

$$\sum_{\substack{\deg v=1 \\ \chi_v \text{ 非分歧}}} \chi_v(\pi_v)$$

正好是所给的特征和, 从而可以应用推论 3 的估计.

从上面讨论可以看出, 定理 2 的证明用到了类域论, 但事实上, 定理 2 的证明并不一定要用类域论, W. Schmidt 在参考文献 [8] 中给出了一个不用类域论的证明.

§2 Weil 的特征和估计

在这一节中, k 仍是一个有 q 个元素的有限域, $K = k(t)$ 是 k 上亏格为 0 的有理函数域. 同平常一样, 我们以 ∞ 表示 K 的以 $P_\infty(t) = 1/t$ 为局部单值化参数的位. 对 K 中一个非零有理函数 $f(t)$, 我们用 $\operatorname{supp} f$ 表示 K 中一些位 (包括 ∞) 的集合, 在这些位处, f 或者有零点或者是极点. 显然, 对任意

$$x \in \mathbf{P}^1(k) = k \bigcup \{\infty\}, \quad f(x) \in \mathbf{P}^1(k).$$

设 χ 是 $k^\times$ 的一个阶 $d > 1$ 的乘法特征标, 令 $\chi(0) = \chi(\infty) = 0$. 我们将 χ 扩展为 $\mathbf{P}^1(k)$ 上的函数, 从而 $\chi(f(x))$ 对任意的 $x \in \mathbf{P}^1(k)$ 均有定义. 又设 ψ 为 k 的加法特征标, $g(t)$ 是 k 上次数为 n 的多项式, 则 $\psi(g(x))$ 对任意 $x \in k$ 均有定义.

1948 年, A. Weil 在参考文献 [9] 中给出下面一些特征和的估计.

定理 3 设 χ, ψ, f 和 g 同上, m 是 $\operatorname{supp} f$ 中异于 ∞ 的所有位的总次数.

(1) 若 $\operatorname{div} f \notin d \cdot \operatorname{Div}(K)$, 则

$$\left|\sum_{x \in P^1(k)} \chi(f(x))\right| \leq (m-1)\sqrt{q};$$

(2) 若 $q > n$ 且 $(n, q) = 1$, 则

$$\left|\sum_{x \in k} \psi(g(x))\right| \leq (n-1)\sqrt{q};$$

(3) 假设 $\operatorname{div} f \notin d \cdot \operatorname{Div}(K)$, 或者 $q > n$ 且 $(n, q) = 1$, 则

$$\left|\sum_{x \in k} \chi(f(x))\psi(g(x))\right| \leq (m+n-1)\sqrt{q}.$$

我们将从下面这个定理来导出定理 3. 对 K 的每个异于 ∞ 的位 v, 固定局部单值化元素 π_v 为 $k[t]$ 中的一个首一不可约多项式, 其根构成 v. 此外, 取定 $\pi_\infty = 1/t$.

定理 4 设 χ, ψ, f 和 g 同上, 进一步假定 $g(0) = 0$. 则

(1) 存在 K 的一个伊代尔类特征标 ω, 使得

(a) ω 在 $\operatorname{supp} f$ 外是非分歧的;

(b) 设 v 是一个不在 $\operatorname{supp} f$ 中的位, 若 $v \neq \infty$, 则

$$\omega_v(\pi_v) = \chi\left(\prod_{j=1}^{\deg v} f(\beta_{j,v})\right),$$

其中 $\beta_{j,v}$ 跑遍 π_v 的所有根; 若 $v = \infty$, 则我们有

$$\omega_\infty(\pi_\infty) = \chi(f(\pi_\infty)).$$

(c) 设 $\operatorname{div} f = \sum_v a_v v$. 则 ω 的前导子是 $\sum_v v$, 其中 v 跑遍所有使得 $d \nmid a_v$ 的位.

(2) 存在 K 的一个在 ∞ 外非分歧的伊代尔类特征标 η, 使得

对每个 $v \neq \infty$,

$$\eta_v(\pi_v) = \psi\left(\sum_{1 \leq j \leq \deg v} g(\beta_{j,v})\right),$$

其中 $\beta_{j,v}$ 跑遍 π_v 的所有根. 进一步, 若 $\deg g = n$ 与 q 互素, 则 η 的前导子为 $(n+1)\infty$.

首先我们假定定理 4 成立来证明定理 3. 给出 χ 和 f 同定理 3, 设 ω 同定理 4. 命

$$S = \{v \in \operatorname{supp} f : d \mid a_v\}.$$

从 $\operatorname{div} f$ 的条件已知 ω 有一个非平凡的前导子

$$\operatorname{cond} \omega = \sum_{v \in \operatorname{supp} f - S} v.$$

以 m' 表示 $\operatorname{cond} \omega$ 的次数, 由推论 3 得

$$\left|\sum_{\substack{\deg v = 1 \\ \omega_v \text{ 非分歧}}} \omega_v(\pi_v)\right| \leq (m' - 2)\sqrt{q}.$$

由此导出

$$\left|\sum_{\substack{\deg v = 1 \\ v \notin \operatorname{supp} f}} \omega_v(\pi_v)\right| \leq \left(m' + \sum_{v \in S} \deg v - 2\right)\sqrt{q}.$$

在一个有 $\pi_v = t - a$ 的位 $v \notin \operatorname{supp} f$ 处, 我们有

$$\omega_v(\pi_v) = \chi(f(a)),$$

这一公式对 $v = \infty \notin \operatorname{supp} f$ 也成立. 进一步, 在其余的点 $b \in \mathbf{P}^1(k)$ 处, 由定义知, $\chi(f(b)) = 0$. 于是上面不等式可以化为

$$\left|\sum_{x \in \mathbf{P}^1(k)} \chi(f(x))\right| \leq \left(m' + \sum_{v \in S} \deg v - 2\right)\sqrt{q}.$$

最后，注意到

$$m' + \sum_{v \in S} \deg v = \begin{cases} m, & 若 \infty \notin \operatorname{supp} f, \\ m+1, & 若 \infty \in \operatorname{supp} f, \end{cases}$$

于是上面不等式右边 $\le (m-1)\sqrt{q}$. 由此定理 3 的第一个断言得证.

为了证明第二个断言，我们假定 $g(0)=0$. 设 η 为定理 4 (2) 中由 ψ 和 g 构造出的 K 的伊代尔类特征标. 有关 n 的条件导出 η 的前导子 $\operatorname{cond} \eta = (n+1)\infty$, 其次数是 $n+1$. 由推论 3 知

$$\left| \sum_{\substack{\deg v = 1 \\ v \neq \infty}} \eta_v(\pi_v) \right| \le (n-1)\sqrt{q}.$$

又在一个 $\neq \infty$ 的次数为 1 的位 v 处，我们有

$$\pi_v = t - a \quad 和 \quad \eta_v(\pi_v) = \psi(g(a)).$$

于是上面那个不等式可改写为

$$\left| \sum_{x \in k} \psi(g(x)) \right| \le (n-1)\sqrt{q}.$$

由此定理 3 (2) 得证.

为了证明第三个断言，我们同样假定 $g(0)=0$. 考虑伊代尔类特征标 $\xi = \omega\eta$, 其中 ω 和 η 同上. 当 $\operatorname{div} f \notin d \cdot \operatorname{Div}(K)$ 时，ω 在某个位 $v \neq \infty$ 处分歧，于是 ξ 也是分歧的，且

$$\operatorname{cond} \xi \le \sum_{\substack{v \in \operatorname{supp} f \\ v \neq \infty}} v + (n+1)\infty.$$

若 ξ 在 ∞ 处分歧，则 $\deg \operatorname{cond} \xi \le m+n+1$, 并且由推论 3 知

$$\left| \sum_{\substack{\deg v = 1 \\ \xi_v \text{ 非分歧}}} \xi_v(\pi_v) \right| = \left| \sum_{x \in k} \chi(f(x))\psi(g(x)) \right| \le (m+n-1)\sqrt{q};$$

若 ξ 在 ∞ 处非分歧，则 $\deg \operatorname{cond} \xi \le m$, $\omega_\infty = 1$, 以及 $\eta = 1$. 同样利用推论 3 得

$$\left|\sum_{\substack{\deg v=1 \\ \xi_v \text{ 非分歧}}} \xi_v(\pi_v)\right| = \left|\sum_{x\in k}\chi(f(x))\psi(g(x)) + 1\right| \le (m-2)\sqrt{q}.$$

这些都导出 (3). 最后，当 $\operatorname{div} f \in d \cdot \operatorname{Div}(K)$ 时，ω 是平凡的. 于是

$$\left|\sum_{x\in k}\chi(f(x))\psi(g(x))\right| = \left|\sum_{\substack{x\in k \\ f(x)\in k^\times}} \psi(g(x))\right|.$$

结合 (2) 即得所需不等式. 这样，定理 3 得证.

注 若 $n \ge q$, 则定理 3 的 (2) 和 (3) 显然成立. 利用 ψ 和 g 定义的特征标 η, 或者满足

$$2\infty \le \operatorname{cond} \eta \le (n+1)\infty.$$

或者它在 I_K 上平凡. 当 η 非平凡时，估计 (2) 是成立的. 此外，当 $g(t)$ 是一个 t 的单项式时，(2) 可以用更容易的方法证明.

习题 1 设 $g(t) = ct^n$, $t \in k^\times$. 利用 Gauss 和的知识证明

$$\left|\sum_{x\in k}\psi(g(x))\right| \le (n-1)\sqrt{q}.$$

现在我们来证明定理 4. 首先，不失一般性，我们可设 $f(t) = cf_1(t)/f_2(t)$ 是 k 中非零常数 c 乘以 $k[t]$ 中两个首一且互素的多项式之商，则

$$f(t) = c\prod_{i=1}^{m}(t-\alpha_i)^{a_i},$$

其中 α_i 互不相同，a_i 为非零整数.

对给定的 χ 和 f, 我们如下定义 $I_K/K^\times$ 的特征标 ω: 在一个非 ∞ 且不在 $\operatorname{supp} f$ 中的位 v 处, 定义 ω_v 在 $\mathcal{U}_v$ 上平凡, 并且

$$\omega_v(\pi_v) = \chi\left(\prod_{j=1}^{\deg v} f(\beta_{j,v})\right),$$

其中 $\beta_{j,v}$ 跑遍 π_v 的所有的根. 若位 $v = \infty \notin \operatorname{supp} f$, 则

$$\deg f_1 = \deg f_2.$$

从而 $f(\infty) = c$ 且 $\deg f = 0$. 此时定义 ω_∞ 在 $\mathcal{U}_\infty$ 上为 1, 应有

$$\omega_\infty(\pi_\infty) = \chi(f(\infty)) = \chi(c).$$

于是, 我们定义了一个在下述的伊代尔上的非分歧特征标 ω: 这些伊代尔在 $\operatorname{supp} f$ 中的位上平凡. 这样的伊代尔全体构成了 I_K 的一个子群, 记作 $\prod'_{v\notin \operatorname{supp} f} K_v^\times$. 通过命 ω 在 $\prod_{v\in \operatorname{supp} f}(1+\mathfrak{p}_v)$ 上取值 1 可把 ω 扩充为

$$I' = \prod_{v\notin \operatorname{supp} f}{}' K_v^\times \prod_{v\in \operatorname{supp} f}(1+\mathfrak{p}_v)$$

上的一个特征标. 由于 $I_K = K^\times \cdot I'$, 所以 ω 可以扩充为 $I_K/K^\times$ 上的一个伊代尔类特征标的充要条件是: 它在 $K^\times \bigcap I'$ 上平凡. 为验证这一点, 任取 $h(t) \in K^\times \bigcap I'$. 设 $h(t) = h_1(t)/h_2(t)$ 为 $k[t]$ 中两个互素多项式之商, 则当 $v \in \operatorname{supp} f$ 且 $v \neq \infty$ 时, $h_1(t)$ 和 $h_2(t)$ 均为 K_v 中单位, 且

$$h_1(t) \equiv h_2(t) \,(\mathrm{mod} \pi_v).$$

这表明 $h_1(t) - h_2(t)$ 可被

$$P(t) := \prod_{\substack{v\in \operatorname{supp} f\\ v\neq\infty}} \pi_v(t) \in k[t]$$

整除. 因此, 对任意的 $i = 1, 2, \cdots, m$, $h_1(\alpha_i) = h_2(\alpha_i) \neq 0$, 即 $h(\alpha_i) = 1$. 若 $\infty \in \operatorname{supp} f$, 则

$$\deg h = \deg h_1 - \deg h_2 = 0,$$

且 h_1, h_2 有相同的首项系数. 利用对 h 的选取, 我们有

$$\omega_v(\pi_v) = \chi(c)^{\deg v}\chi\left(\prod_{i=1}^{m}\pi_v(\alpha_i)^{a_i}\right)\chi(-1)^{\deg v \deg f}$$

和 $\deg f \deg h = 0$. 于是由定义可得

$$\begin{aligned}\omega(h) &= \prod_v \omega_v(h) = \prod_{v \notin \operatorname{supp} f} \omega_v(h) \\ &= \chi(c)^{-\deg h} \prod_{\substack{v \\ \pi_v \text{ 整除 } h_1 \text{ 或 } h_2}} \omega_v(h) \\ &= \chi\left(\prod_{i=1}^{m} h(\alpha_i)^{a_i}\right) = \chi(1) = 1.\end{aligned}$$

这样我们就得到了一个阶 $\leq d$ 的 $I_K/K^{\times}$ 的伊代尔类特征标 ω.

设

$$\operatorname{div} f = \sum_{v \in \operatorname{supp} f} a_v v.$$

下面我们将证明 ω 在使得 $d \nmid a_v$ 的位 $v \in \operatorname{supp} f$ 处分歧, 而在 $\operatorname{supp} f$ 中其他位处, ω 非分歧. 设 $v \in \operatorname{supp} f$ 且 $v \neq \infty$. 假设

$$\pi_v(t) = \prod_{i=1}^{\deg v}(t - \alpha_i),$$

使得 $i = 1, 2, \cdots, \deg v$ 时, $a_i = a_v$. 我们已经知道 K_v 的剩余类域 κ_v 是 $k(\alpha_1)$, π_v 的根均为 α_1 关于 $\mathrm{Gal}(\kappa_v/k)$ 的共轭. 于是存在多项式 $x(t) \in k[t]$, 使得 $x(\alpha_1)$ 生成 $\kappa_v^{\times}$, 进而 $k^{\times}$ 可由

$$\mathrm{N}_{\kappa_v/k}(x(\alpha_1)) = \prod_{i=1}^{\deg v} x(\alpha_i)$$

生成. 利用中国剩余定理, 我们可以找到多项式 $h_1(t)$ 和 $h_2(t) \in k[t]$, 使得

$$h_1(t) \equiv x(t), \quad h_2(t) \equiv 1 \pmod{\pi_v},$$

$$h_1(t) \equiv h_2(t) \equiv 1 \pmod{\pi_w}, \quad w \in \operatorname{supp} f,\ w \neq v, \infty.$$

如果必要，在 $h_1(t)$ 和 $h_2(t)$ 上添加 $P(t)$ 的适当倍数，这样我们总可假定 h_1 和 h_2 有同样的次数和首项系数．令

$$h(t) = h_1(t)/h_1(t) \in K^{\times}.$$

则

$$h(t) \equiv x(t) \pmod{\pi_v},$$

$$h(t) \equiv 1 \pmod{\pi_w}, \quad w \in \operatorname{supp} f,\ w \neq v, \infty.$$

从关系式

$$\begin{aligned}
1 = \omega(h(t)) &= \omega_v(h(t)) \prod_{w \notin \operatorname{supp} f} \omega_w(h(t)) \\
&= \omega_v(h(t)) \cdot \chi\left(\prod_{i=1}^{m} h(\alpha_i)^{a_i}\right) \\
&= \omega_v(h(t)) \cdot \chi\left(\prod_{i=1}^{\deg v} h(\alpha_i)\right)^{a_v} = \omega_v(h(t)) \cdot \chi\left(\prod_{i=1}^{\deg v} x(\alpha_i)\right)^{a_v}
\end{aligned}$$

我们可得

$$\omega_v(h(t)) = \chi\left(\prod_{i=1}^{\deg v} x(\alpha_i)\right)^{-a_v}.$$

由于

$$\prod_{i=1}^{\deg v} x(\alpha_i) = \mathrm{N}_{K_v/k}(x(\alpha_1))$$

生成 $k^{\times}$ 且 χ 的阶为 d, 于是当 $d \nmid a_v$ 时， $\omega_v(h(t)) \neq 1$; 另一方面，当 $d \mid a_v$ 时，同样的讨论可以证明，对 $k[t]$ 中任意与 π_v 互素的 $x(t)$, 有 $\omega_v(h(t)) = 1$. 从而 ω_v 在 $K_v^{\times}$ 的单位上平凡，即 ω_v 是非分歧的．最后，如果 $\infty \in \operatorname{supp} f$, 取

$$h_2(t) = 1 + P(t), \quad h_1(t) = 1 + bP(t),$$

其中 $b \in k^\times$, 则 $h(t) = h_2(t)/h_1(t)$ 模 $P(t)$ 同余于 1, 模 $\mathfrak{p}_\infty$ 同余于 b, 从而有

$$1 = \omega(h) = \omega_\infty(h(t)) \prod_{w \notin \text{supp} f} \omega_w(h(t))$$

$$= \omega_\infty(h(t)) \prod_{i=1}^{m} \chi((P(\alpha_i) + b^{-1})/h_1(\alpha_i))^{a_i}$$

$$= \omega_\infty(b) \cdot \chi(b)^{-\deg f} = \omega_\infty(b) \cdot \chi(b)^{a_\infty}.$$

进而可知, ω_∞ 在 $\mathcal{U}_\infty$ 上平凡的充要条件是 $d \nmid a_\infty$. 这就证明了定理 4 的第一个断言.

为证明定理 4 的第二个断言, 给定 $k[t]$ 中一个常数项为 0 的多项式 $g(t)$ 和特征标 ψ. 利用 g 和 ψ, 我们将如下构造一个 $I_K/K^\times$ 的一个伊代尔类特征标 η. 首先, 在 $K_\infty^\times$ 上定义 η_∞. 命 η_∞ 在 $\pi_\infty = 1/t$ 和 $k^\times$ 上平凡, 对多项式

$$h(x) = 1 + a_1 x + \cdots + a_u x^u = (1 - \gamma_1 x) \cdots (1 - \gamma_u x),$$
$$a_i \in k, \ \gamma_i \in \overline{k}$$

定义

$$\eta_\infty(h(\pi_\infty)) = \overline{\psi}(g(\gamma_1) + \cdots + g(\gamma_u)),$$

这里 $\overline{\psi}$ 表示 ψ 的复共轭. 由于 $g(0) = 0$, 而且如果必要, 我们可以在 $h(x)$ 上添加一些系数为 0 的项, 所以我们总可假定 $u \geq n$. 设

$$g(t) = b_n t^n + \cdots + b_1 t,$$

其中 $b_i \in k$ 且 $b_n \neq 0$, 则

$$g(\gamma_1) + \cdots + g(\gamma_u) = b_n s_n + b_{n-1} s_{n-1} + \cdots + b_1 s_1,$$

这里

$$s_i = \sum_{j=1}^{u} \gamma_j^i, \quad i = 1, 2, \cdots, n.$$

反复利用 Newton 等式 (参见参考文献 [4])

$$s_i + a_1 s_{i-1} + a_2 s_{i-1} + \cdots + a_{i-1} s_1 + i a_i = 0,$$

可以看到，$g(\gamma_1)+\cdots+g(\gamma_u)$ 是系数在 k 中，变数为 $a_1,\cdots,a_n$ 的多项式，并且 $-nb_na_n$ 是唯一含有 a_n 的项. 换句话说，存在 k 上的一个 $n-1$ 元多项式 $\widetilde{g}$, 使得

$$g(\gamma_1)+\cdots+g(\gamma_u)=-nb_na_n+\widetilde{g}(a_1,\cdots,a_{n-1}).$$

特别地，从上面看出，$g(\gamma_1)+\cdots+g(\gamma_u)\in k$. 因此 $\eta_\infty(h(\pi_\infty))$ 是有意义的，同时，这也证明了 $\eta_\infty(h(\pi_\infty))$ 只依赖于 $a_1,\cdots,a_n$. 换句话说，若有 $k[t]$ 中两个常数项均为 1 的多项式 $h_1(t)$ 和 $h_2(t)$, 它们的前 n 项相同，则

$$\eta_\infty(h_1(\pi_\infty))=\eta_\infty(h_2(\pi_\infty)).$$

因此，$1+\mathfrak{p}_\infty^{n+1}$ 中 π_∞ 的任意多项式在 η_∞ 作用下的值为 1. 将 η_∞ 连续地扩展到 $1+\mathfrak{p}_\infty$ 上，使得它在 $1+\mathfrak{p}_\infty^{n+1}$ 上平凡. 进而由

$$\eta_\infty(h_1(\pi_\infty)h_2(\pi_\infty))=\eta_\infty(h_1(\pi_\infty))\eta_\infty(h_2(\pi_\infty)),$$

$$h_1,h_2\in k[t],\ \text{且}\ h_1(0)=h_2(0)=1$$

知，η_∞ 是 $1+\mathfrak{p}_\infty$ 的一个特征标. 再利用分解式

$$K_\infty^\times=\langle\pi_\infty\rangle k^\times(1+\mathfrak{p}_\infty),$$

并结合 η_∞ 的定义，我们就得到 $K_\infty^\times$ 的一个特征标 η_∞.

通过命 η 在 $\prod\limits_{v\neq\infty}\mathcal{U}_v$ 上取值为 1 可以把 η_∞ 扩展成 $K_\infty^\times\prod\limits_{v\neq\infty}\mathcal{U}_v$ 上的特征标. 由于

$$K^\times\bigcap\left(K_\infty^\times\prod_{v\neq\infty}\mathcal{U}_v\right)=k^\times,$$

以及 η_∞ 在 $k^\times$ 上平凡，我们可以进一步将 η 扩展为 $I_K/K^\times$ 上的特征标. 这里用到了分解式

$$I_K=K^\times\cdot K_\infty^\times\prod_{v\neq\infty}\mathcal{U}_v.$$

显然，这样得到的特征标 η 是有限阶的.

假定 $(q,n)=1$, 我们断言 η 在 ∞ 处分歧. 事实上, 从前面分析看出, 当 $h(x)=1+a_nx^n$, $a_n\in k$ 时

$$\eta_\infty(h(\pi_\infty))=\overline{\psi}(-nb_na_n).$$

由于 $(q,n)=1$, $b_n\neq 0$, 故当 a_n 跑遍 k 中元素时, $-nb_na_n$ 亦跑遍 k 中的元. 又因 ψ 是非平凡的, 从而 η 的前导子

$$\operatorname{cond}\eta=(n+1)\infty,$$

其次数是 $n+1$.

最后, 注意到在一个具有局部单值化元素

$$\pi_v=\prod_{j=1}^{\deg v}(t-\beta_{j,v})=t^{\deg v}\prod_{j=1}^{\deg v}(1-\beta_{j,v}\pi_\infty)$$

且 $\neq\infty$ 的位 v 处, 由

$$1=\eta(\pi_v)=\eta_v(\pi_v)\eta_\infty(\pi_v)=\eta_v(\pi_v)\overline{\psi}\left(\sum_{j=1}^{\deg v}g(\beta_{j,v})\right)$$

可得 $\eta(\pi_v)=\psi\left(\sum_{j=1}^{\deg v}g(\beta_{j,v})\right)$. 这就证明了断言 (2). 定理 4 得证.

习题 2 设 K 是 k 上的有理函数域, S 是由有限多个 K 的位组成的集合, 证明, 对任意自然数 n_v 有

$$I_K=\left({\prod_{v\notin S}}'K_v^\times\prod_{v\in S}(1+\mathfrak{p}_v^{n_v})\right)K^\times.$$

推论 4 设 $f(t)$ 是 k 上首一多项式, 且 $f(t)$ 有 m 个不同的根. 如果 f 不是 $k[t]$ 中一个多项式的 d 次幂, 则对 $k^\times$ 的一个 d 阶特征标 χ, 有

$$\left|\sum_{x\in k}\chi(f(x))\right|\leq(m-1)\sqrt{q}.$$

利用定理 3, 我们还可导出一个关于 Kloosterman 和的估计.

推论 5(Weil) 设 $b, c \in k$, 且它们不同时为 0. 假定 q 是奇数, 则对 k 的任意非平凡加法特征标 ψ, 有

$$\left|\sum_{x\in k^{\times}} \psi(bx + cx^{-1})\right| \leq 2\sqrt{q}.$$

特别地, 当 $k = \mathbf{Z}/p\mathbf{Z}$ 时有

$$\left|\sum_{x=1}^{p-1} \mathrm{e}^{2\pi \mathrm{i}(bx+cx^{-1})/p}\right| \leq 2\sqrt{p},$$

其中 p 是一个奇素数.

证 若 b 和 c 中有一个为 0, 则另一个不为 0. 于是

$$\sum_{x\in k^{\times}} \psi(bx + cx^{-1}) = -1$$

显然满足不等式, 因此我们现在假定 $bc \neq 0$. 设 $a = 4bc$. 命 $y = bx + cx^{-1}$, 则

$$y^2 - a = (bx - cx^{-1})^2$$

是一个平方. 容易验证: 可以且只可以在 $x_1 = x_2$ 或 $x_1x_2 = c/d$ 时, $bx_1 + cx_1^{-1} = bx_2 + cx_2^{-1}$ 成立. 此外, 方程 $x_1^2 = c/b$ 可解的充要条件是 bc 是个平方数. 这等价于 $y^2 - a = 0$ 是可解的.

设 χ 是 $k^{\times}$ 的一个二次特征标, 它在 $k^{\times}$ 的平方数处取值 1, 在非平方数处取值 -1. 设

$$f(t) = t^2 - a, \quad g(t) = t.$$

由定理 3 (3) 得

$$\left|\sum_{y\in k} \psi(y)\chi(y^2 - a)\right| \leq 2\sqrt{q}.$$

此外, 从 ψ 的非平凡性可以导出 $\sum\limits_{y\in k} \psi(y) = 0$, 从而推论 5 可以由关系式

$$\sum_{x\in k^{\times}} \psi(bx + cx^{-1}) = \sum_{y\in k} \psi(y)(\chi(y^2 - a) + 1)$$

导出，为证明此关系式，我们分两种情况来讨论.

情形 1： bc 不是平方数. 此时， y^2-a 恒不为 0, 并且

$$\sum_{y\in k}\psi(y)(\chi(y^2-a)+1)=2\sum_{\substack{y\in k\\ y^2-a\in k^{\times 2}}}\psi(y).$$

设 $y^2-a=u^2\in k^{\times 2}$, 则

$$(y+u)(y-u)=a=4bc\neq 0,$$

于是我们可找到 $x\in k^\times$, 使得 $y+u=2bx$. 从而 $y-u=2cx^{-1}$. 这表明 $y=bx+cx^{-1}$. 另一方面，我们已知，当 y 是形如 $bx+cx^{-1}$ 的数时， y^2-a 是一个非零平方数. 进而，由 x 到 y 的映射是 2 对 1 的，这就表明

$$2\sum_{\substack{y\in k\\ y^2-a\in k^{\times 2}}}\psi(y)=\sum_{x\in k^\times}\psi(bx+cx^{-1}).$$

情形 2： $bc=d^2\in k^{\times 2}$. 此时， $y^2-a=0$ 有

$$y=\pm 2d=\pm\left(b\frac{d}{b}+c\frac{b}{d}\right)$$

这两个解. 于是我们有

$$\sum_{y\in k}\psi(y)(\chi(y^2-a)+1)=2\left(\sum_{\substack{y\neq\pm 2d\\ y^2-a\in k^{\times 2}}}\psi(y)\right)+\psi(2d)+\psi(-2d).$$

利用情形 1 中的讨论可知，当 $y\neq\pm 2d$ 且 y^2-a 是个平方数时，方程 $y=bx+cx^{-1}$ 关于 x 在 $k^\times$ 中恰有两个解；而当 $y=\pm 2d$ 时，该方程只有一个解 $x=\pm d/b$. 由此我们可以导出所需公式.

习题 3 利用构造一个导子 cond $\chi=2\cdot 0+2\cdot\infty$ 的 $I_K/K^\times$ 的伊代尔类特征标 χ, 以及关系式

$$\sum_{\substack{\deg v=1\\ v\neq 0,\infty}}\chi_v(\pi_v)=\sum_{x\in k^\times}\psi(bx+cx^{-1})$$

来证明推论 5.

下面我们给出一个定理 3 在 Diophantine 方程中的应用，读者可以同时参见参考文献 [9]. 同前面一样， k 仍是一个有 q 个元素的有限域. 给定 k 上多项式 $f_1(x),\cdots,f_r(x)$, 考虑方程组

$$y_1^{n_1}=f_1(x),\quad \cdots,\quad y_r^{n_r}=f_r(x).$$

我们将计算该方程组的解 $(x,y_1,\cdots,y_r)\in k^{r+1}$ 的个数 N. 设 $d_i=\gcd(n_i,q-1)$, 首先我们看到 $y_i^{n_i}=f_i(x)$ 与 $y_i^{d_i}=f_i(x)$ 有相同的解数. 为简化计算，我们假定，当 $j\,|\,d_i$ 且 $j\neq d_i$ 时， $f_i(x)^j$ 是首一多项式且不是其他多项式的 d_i 次幂. 此外， f_i 两两互素. 同第二章 §1 中一样，以 $\mathrm{N}_i(u)$ 表示 $y^{d_i}=u$ 的解数，于是 N_i 可以用特征和来表示

$$\mathrm{N}_i=\sum_{\chi}\chi,$$

其中 χ 的求和范围是 $k^\times$ 的所有阶可整除 d_i 的特征标. 取定 $\widehat{k^\times}$ 的一个生成元 χ, 我们有

$$\mathrm{N}_i=\sum_{j=0}^{d_i-1}\chi^{je_i},$$

其中 $e_i=(q-1)/d_i$. 于是

$$\begin{aligned}N&=\sum_{x\in k}\mathrm{N}_1(f_1(x))\cdots\mathrm{N}_r(f_r(x))\\&=\sum_{x\in k}\sum_{j_1=0}^{d_1-1}\cdots\sum_{j_r=0}^{d_r-1}\chi^{j_1e_1}(f_1(x))\cdots\chi^{j_re_r}(f_r(x))\\&=q+\sum_{x\in k}\ \sideset{}{'}\sum_{0\le j_i\le d_i-1}\chi(f_1^{j_1e_1}\cdots f_r^{j_re_r}),\end{aligned}$$

上式中和号 $\sum'$ 表示去掉 $j_i=j_2=\cdots=j_r=0$ 这一项. 而第一项 q 恰由此项产生，它是 N 的主项. 当 $0\le j_i\le d_i-1$ 且并非所有 $j_r=0$ 时，对指标组 $J=(j_1,\cdots,j_r)$, 多项式

$$f^J(x)=f_1(x)^{j_1e_1}\cdots f_r(x)^{j_re_r}$$

是个首一多项式并且不是任一多项式的 $q-1$ 次幂. 于是利用推论 4 可得

$$\left|\sum_{x\in k}\chi(f^J(x))\right| \leq (m-1)\sqrt{q},$$

其中 m 是 $f_1(x)\cdots f_r(x)$ 的不同根的数目. 这表明

$$|N-q| \leq (d_1\cdots d_r-1)(m-1)\sqrt{q}.$$

定理 5(Schmidt[9]) 设 $f_1(x),\cdots,f_r(x)$ 是 $k[t]$ 中两两互素的首一多项式, 设 N 是联立方程组

$$y_1^{n_1}=f_1(x), \quad \cdots, \quad y_r^{n_r}=f_r(x)$$

在 k^{r+1} 中解的个数. 又设 $d_i=\gcd(n_i,q-1)$. 此外我们还假定当 $j\,|\,d_i$ 且 $j\neq d_i$ 时, $f_i(x)^j$ 不是任一多项式的 d_i 次幂. 那么

$$|N-q| \leq (d_1\cdots d_r-1)(m-1)\sqrt{q},$$

这里 m 是方程 $f_1(x)\cdots f_r(x)=0$ 的不同的解的数目. 特别地, 当 q 充分大时, 我们有 $N=q+O(\sqrt{q})$.

设 p 是个奇素数, 将定理 5 应用于 $k=\mathbf{Z}/p\mathbf{Z}$, $f_1(x)=x+1,\cdots,f_r(x)=x+r$, 以及 $n_1=n_2=\cdots=n_r=2$ 这种特殊情况. 此时所要研究的方程组是

$$y_1^2=x+1, \quad y_2^2=x+2, \quad \cdots, \quad y_r^2=x+r.$$

对这一方程组的每一个解 $x\in k$, 对应的 $x+1,\cdots,x+r$ 同时都是 k 中的平方数. 如果 $x+1,\cdots,x+r$ 中有一个为 0, 则由此可导出方程组的 2^{r-1} 个解. 以 N_0 表示该方程组的解集中那些使得 $f_1(x)\cdots f_r(x)=0$ 的解 $(x,y_1,\cdots,y_r)$ 的个数, 则 $\mathrm{N}_0\leq r2^{r-1}$. 在剩余的解里面, 对每个 x 值, 都有两个 y_i 的值与之对应, 即对应了方程组的 2^r 个解, 我们以 R_r 表示 k 中那些使 $x+1,\cdots,x+r$ 为二次剩余的 x 的个数, 则 $N=2^rR_r+\mathrm{N}_0$.

综合上面讨论, 我们就得到了下面的推论.

推论 6　当素数 p 充分大时，$\mathbf{Z}/p\mathbf{Z}$ 中使 $x+1, x+2, \cdots, x+r$ 均为模 p 的二次剩余的元素 x 的个数

$$R_r = \frac{p}{2^r} + O(\sqrt{p}).$$

很明显，如果把 $1,2,\cdots,r$ 换成另外 r 个互不相同的数，也有同样的结论成立.

§3　特征和的估计

在这一节中，我们将给出更多特征和的估计，它们在数论及其组合学理论中都有十分好的应用．在本书的第九章中我们将涉及这些特征和估计的一些应用．本节的结果均选自参考文献 [8].

同前几节一样，设 k 是有 q 个元素的有限域，k_n 表示 k 在其某个代数闭包 $\bar{k}$ 中的 n 次扩张．设 N_n 是范映射

$$\mathrm{N}_{k_n/k} : k_n^\times \to k^\times$$

的核，又取 $t \in k_n$ 使得 $k_n = k(t)$. 此外，我们假定 $n \geq 2$. 令

$$S_n = \left\{ \frac{t^q + a}{t + a} : a \in k \bigcup \{\infty\} = \mathbf{P}^1(k) \right\},$$

其中，当 $a = \infty$ 时，∞/∞ 被指定为 1. 以 σ 表示 $\mathrm{Gal}(k_n/k)$ 中将 x 映为 x^q 的 Frobenius 映射，于是 $t^q + a = \sigma(t+a)$, S_n 含于 N_n 中.

定理 6　对 N_n 的每个非凡特征标 χ，有

$$\left| \sum_{s \in S_n} \chi(s) \right| \leq (n-2)\sqrt{q}.$$

证　设 $P(T)$ 是 t 在域 k 的极小多项式，w 是由 $P(T)$ 对应的 $K = k(T)$ 的位．则 $\deg w = n$ 且 $P(T)$ 是 K_w 的局部单值化元素．将 T 映为 t 的从 O_w 到 k_n 的 k-同态显然是个满射，并且其核是由 $P(T)$ 生成的理想，即 $\mathfrak{p}_w$. 由此我们得到一个同态 $O_w/\mathfrak{p}_w \cong k_n$,

这诱导出同构

$$\mathcal{U}_w/(1+\mathfrak{p}_w) \cong k_n^\times.$$

利用第一章定理 3 知, $N_n = \{\sigma(x)/x : x \in k_n^\times\}$. 由此看出, 映 x 为 $x/\sigma(x)$ 的从 $k_n^\times$ 到 N_n 的同态诱导出同构 $k_n^\times/k^\times \cong N_n$. 综上所述, 我们得到

$$\mathcal{U}_w/k^\times(1+\mathfrak{p}_w) \cong k_n^\times/k^\times \cong N_n.$$

因此, 由 N_n 的一个特征标 χ 可以导出 $\mathcal{U}_w$ 的一个在 $k^\times(1+\mathfrak{p}_w)$ 上平凡的特征标 ω_w, 并且当 χ 是非平凡时, ω_w 的前导子是 w. 通过命 ω 在 $\langle\pi_\infty\rangle \prod\limits_{v\neq\omega} \mathcal{U}_v$ 上平凡把 ω_w 扩充为 $\langle\pi_\infty\rangle \prod\limits_{v} \mathcal{U}_v$ 上的特征标 ω. 又因

$$\left(\langle\pi_\infty\rangle \prod_v \mathcal{U}_v\right) \bigcap K^\times = k^\times \quad \text{和} \quad \omega$$

在 $k^\times$ 上平凡, 我们可以把 ω 扩张为 I_K 上的特征标, 此时只需命 ω 在 $K^\times$ 上平凡即可做到这一点. 于是 ω 就成为 $I_K/K^\times$ 的一个有限阶伊代尔类特征标, 其导子 $\operatorname{cond}\omega = w$. 利用推论 3 可得

$$\left|\sum_{\deg v=1} \omega_v(\pi_v)\right| \le (n-2)\sqrt{q}.$$

在 $v=\infty$ 处,

$$\omega_\infty(\pi_\infty) = 1 = \chi(1);$$

在局部单值化元素 π_v 为 $T+a$ 的位 v 处, 由 ω 的构造可得

$$\omega_v(\pi_v) = \omega_w(T+a)^{-1} = \chi\left(\frac{t+a}{\sigma(t+a)}\right)^{-1} = \chi\left(\frac{t^q+a}{t+a}\right).$$

由此定理 6 得证.

接下来, 命

$$S_n' = \left\{\frac{1}{t+a} : \ a \in k \bigcup \{\infty\}\right\}.$$

当 $a=\infty$ 时, $1/\infty$ 被指定为 0.

定理 7 对 k_n 的一个非平凡加法特征标 ψ, 有

$$\left|\sum_{s\in S_n'}\psi(s)\right|\leq(2n-2)\sqrt{q}.$$

证 取 $P(T), w$ 和 K 与定理 5 的证明中的 $P(T), w$ 和 K 意义相同. 同样, 将 T 映为 t 的同态诱导出同构 $\mathcal{O}_w/\mathfrak{p}_w\cong k_n$. 由于 k_n 中元素均为 $T^{q^n}-T$ 在 $\bar{k}$ 中的根, 所以多项式 $T^{q^n}-T$ 在 k 上可以分解为一些次数能整除 n 的不可约首一多项式的积. 特别地, t 的最小多项式 $P(T)\,\|\,T^{q^n}-T$, 即 $P(T)$ 整除 $T^{q^n}-T$ 且 $P(T)^2\nmid T^{q^n}-T$. 于是我们可取 π_w 为 $T^{q^n}-T$. 在第四章 §2 中我们看到, 利用 Hensel 引理, k_n 中的非零元可以提升为 K_w 中的 q^n-1 次单位根, 以 U 表示它们构成的群, 则 U 含于单位群 $\mathcal{U}_w$ 中, 事实上,

$$\mathcal{U}_w=U(1+\mathfrak{p}_w).$$

因此 $\mathcal{U}_w/U(1+\mathfrak{p}_w^2)$ 同构于 $(1+\mathfrak{p}_w)/(1+\mathfrak{p}_w^2)$, 而后者在映射 $1+\pi_w h\longmapsto h$ 下同构于 $\mathcal{O}_w/\mathfrak{p}_w$. 利用映射 $T\longmapsto t$, 我们将 $\mathcal{U}_w/U(1+\mathfrak{p}_w^2)$ 与 k_n 等同起来. 于是 k_n 的一个非平凡特征标 ψ 对应了 $\mathcal{U}_w$ 的一个在 $\mathcal{U}(1+\mathfrak{p}_w^2)$ 上平凡, 前导子为 $2w$ 的特征标 η_w. 同前面一样, 通过让 η 在

$$K^\times\prod_{v\neq w}\mathcal{U}_v\langle\pi_\infty\rangle$$

上平凡把 η_w 扩充为 $I_K/K^\times$ 的一个伊代尔类特征标 η, 从 $k^\times\subset\mathcal{U}$ 以及 η_w 在 $k^\times$ 上平凡可知上面扩充是在可行的. 显然 $\mathrm{cond}\,\eta=2w$, $\mathrm{cond}\eta$ 的次数是 $2n$. 利用推论 3 得

$$\left|\sum_{\deg v=1}\eta_v(\pi_v)\right|\leq(2n-2)\sqrt{q}.$$

又因 $\eta_\infty(\pi_\infty) = 1 = \psi(0)$, 所以上面不等式可化为

$$\left|1 + \sum_{a \in k} \eta_w (T+a)^{-1}\right| \leq (2n-2)\sqrt{q}.$$

剩下的就是证明

$$\eta_w (T+a)^{-1} = \psi\left(\frac{1}{t+a}\right).$$

我们先看看是什么样的 $u \in U$ 和 $h \in O_w$ 使得

$$(T+a)^{-1} \equiv u(1+\pi_w h) \pmod{\mathfrak{p}_w^2}.$$

将此同余式两边乘 q^n 次方得

$$(T+a)^{-q^n} \equiv u^{q^n} \equiv u \pmod{\mathfrak{p}_w^2}.$$

于是

$$\begin{aligned} 1+\pi_w h &\equiv \frac{(T+a)^{q^n}}{(T+a)} \equiv \frac{T^{q^n}+a}{T+a} \\ &\equiv 1 + \pi_w \frac{1}{T+a} \pmod{\mathfrak{p}_w^2}. \end{aligned}$$

换句话说, $\mathcal{U}_w/U(1+\mathfrak{p}_w^2)$ 中的 $(T+a)^{-1}$ 等同于 $O_w/\mathfrak{p}_w$ 中的 $(T+a)^{-1}$. 而这又等同于 k_n 中的 $(t+a)^{-1}$. 于是我们有

$$\eta_w (T+a)^{-1} = \psi\left(\frac{1}{t+a}\right).$$

定理得证.

注意到, 对 $a \in k \bigcup \{\infty\}$, 有

$$\frac{t^q + a}{t+a} = 1 + \frac{t^q - t}{t+a},$$

因此 $S_n = bS_n' + c$, 其中 $b = t^q - t$, $c = 1$. 换句话说, S_n 和 S_n' 是相互的仿射变换. 又因 ψ 在跑遍 k_n 的所有非平凡加法特征标时 ψ^b 也跑遍 k_n 的所有非平凡加法特征标, 所以我们可改写定理 7 为下述定理.

定理 7′ 对 k_n 的任意非平凡加法特征标 ψ, 有

$$\left|\sum_{s\in S_n}\psi(s)\right|\leq(2n-2)\sqrt{q}.$$

考虑 $n=2$ 时的情况. 显然 $S_2\subset N_2$. 不过由于 S_2 与 N_2 的势均为 $q+1$, 因此 $S_2=N_2$. 从而得到

推论 7 对 k_2 的任意非平凡加法特征标 ψ, 有

$$\left|\sum_{x\in N_2}\psi(x)\right|\leq 2\sqrt{q}.$$

通过研究 Frobenius 自同构在一定的平展上同调上的作用, P. Deligne 在参考文献 [3] 中证明了下面的关于广义 Kloosterman 和的估计.

定理 8(Deligne) 对 k_n 的任意非平凡加法特征标 ψ, 有

$$\left|\sum_{x\in N_n}\psi(x)\right|\leq nq^{(n-1)/2}.$$

显然, 推论 7 是定理 8 的特殊情况. 不过, 从上面对此特殊情况的讨论中看出, 此时估计可以从有限域上曲线的 Riemann 猜想得出, 而不必涉及平展上同调的知识.

定理 9 对 $N_n\times k_n$ 的任意非平凡特征标 (χ,ψ), 有

$$\left|\sum_{x\in S_n}\chi(s)\psi(s)\right|\leq(2n-2)\sqrt{q}.$$

证 若 χ 和 ψ 中有一个是平凡的, 那么上面不等式可以由定理 6, 或定理 7′ 得到, 因此下面假定 χ 和 ψ 都是非平凡的. 设 w 是对应于 t 的极小多项式 $P(T)$ 的位, ω 和 η 分别为由 χ 和 ψ^b 按定理 6 和定理 7 证明中的方法所构造的 $I_K/K^\times$ 的伊代尔类特征标. 这里 $b=t^q-t$, 使得

$$S=bS'+1,\qquad K=k(T).$$

注意到 cond $\omega = w$, cond $\eta = 2w$. 因此 $\omega\eta$ 为 $I_K/K^\times$ 有限阶伊代尔类特征标且 cond $\omega\eta = 2w$. 设 v 是有局部单值化元素 $\pi_v = T+a$ 的位，由 ω 和 η 的定义得

$$\omega_v\eta_v(\pi_v) = \omega_w\eta_w(T+a)^{-1} = \chi\left(\frac{t^q+a}{t+a}\right)\cdot\psi^b\left(\frac{1}{t+a}\right)$$

$$= \chi\left(\frac{t^q+a}{t+a}\right)\cdot\psi\left(\frac{t^q+a}{t+a}\right)\psi(-1)$$

和

$$\omega_\infty\eta_\infty(\pi_\infty) = \chi(1)\psi^b(0) = \chi(1)\psi(1)\psi(-1).$$

结合推论 3 即得

$$\left|\sum_{\deg v=1}\omega_v\eta_v(\pi_v)\right| = \left|\sum_{s\in S_n}\chi(s)\psi(s)\psi(-1)\right| \le (2n-2)\sqrt{q}.$$

由此定理得证.

再回到 $n=2$ 的情况，此时 $S_2 = N_2$. 于是此刻的定理 8 变为下述推论.

推论 8 对 $N_2\times k_2$ 的每个非平凡特征标 (χ,ψ), 有

$$\left|\sum_{x\in N_2}\chi(x)\psi(x)\right| \le 2\sqrt{q}.$$

推论中的特征和可以看成 N_2 上的 Gauss 和. 让我们回想一下 N_2 是范映射 $\mathrm{N}_{k_2/k}$ 的核，而范映射可以用 k 上的一个二次型 $q(x,y)$ 来表示，于是 N_2 是由 $q(x,y)=1$ 的解组成的，从而它是个椭圆. 这可以看作双曲线 $xy=1$ 在 k^2 中的"紧形式". 于是推论 8 的一个"分裂"模拟形式应该是

$$\left|\sum_{x\in k^\times}\mu(x)\nu(x^{-1})\psi(bx+cx^{-1})\right|$$

$$= \left|\sum_{x\in k^\times}\mu\nu^{-1}(x)\psi(bx+cx^{-1})\right| \le 2\sqrt{q},$$

其中或者 $\mu\nu^{-1}$ 是 $k^\times$ 的非平凡特征标，或者 $b, c \in k$ 不同时为 0. 注意到，k^2 的特征标可写成 $\psi(bx+cy)\,(b,c \in k^2)$ 的形式 (参见第一章). 下面我们将证明这个模拟形式是正确的. 顺便指出，当 $b=c=1$ 这种特殊的情况是由 Mordell 首先证明的. 此外，当 $\mu\nu^{-1}$ 非平凡时，该和式被称为**扭曲的 Kloosterman 和**.

定理 10 设 ψ 是 k 的一个非平凡加法特征标，假设或者 χ 是 $k^\times$ 的一个非平凡特征标，或者 $(b,c) \in k^2 - \{(0,0)\}$. 则

$$\left|\sum_{x\in k^\times} \chi(x)\psi(bx+cx^{-1})\right| \leq 2\sqrt{q}.$$

证 若 χ 平凡，则此不等式可由推论 5 得出，于是我们总假定 χ 是非平凡的. 此外，若 b 或 c 为 0，则扭曲的 Kloosterman 和变为通常的 Gauss 和，因此其绝对值为 $\sqrt{q}$，上述不等式当然成立. 所以接下来我们还假定 $bc \neq 0$. 我们将利用 χ 和 ψ 来构造一个 $K=k(T)$ 的导子为 $2\cdot 0 + 2\cdot\infty$ 的伊代尔类特征标 ξ. 取 0 处的局部单值化元素为 T. 那么 $\mathcal{U}_0/(1+\mathfrak{p}_0^2)$ 中的任意元素总可写成 $x(1+yT)\,(x\in k^\times, y \in k)$ 的形式. 利用

$$\xi_0(x(1+yT)) = \chi(x)^{-1}\overline{\psi}(cy)$$

来在 $\mathcal{U}_0/(1+p_0^2)$ 上定义 ξ_0; 取 $\pi_\infty = 1/T$, 类似地，$\mathcal{U}_\infty/(1+p_\infty^2)$ 中元素可以写成 $x(1+y\pi_\infty)\ (x\in k^\times, y\in k)$ 的形式，在 $\mathcal{U}_\infty/(1+p_\infty^2)$ 上利用

$$\xi_\infty(x(1+y\pi_\infty)) = \chi(x)\overline{\psi}(by)$$

定义 ξ_∞. 容易验证，ξ_0 和 ξ_∞ 分别是 $\mathcal{U}_0$ 和 $\mathcal{U}_\infty$ 上的特征标. 通过让 ξ 在 $\prod\limits_{v\neq 0,\infty} \mathcal{U}_v\langle\pi_\infty\rangle$ 上平凡，把 ξ_0, ξ_∞ 扩充为 $\prod\limits_v \mathcal{U}_v\langle\pi_\infty\rangle$ 上的特征标 ξ. 由于 ξ 在

$$\left(\prod_v \mathcal{U}_v\langle\pi_\infty\rangle\right) \bigcap K^\times = k^\times$$

上平凡, 所以它可以扩充为 $I_K/K^\times$ 的一个有限伊代尔类特征标, 其前导子显然为 $\operatorname{cond}\xi = 2\cdot 0 + 2\cdot\infty$. 利用推论 3 得

$$\left|\sum_{\substack{\deg v=1\\ v\neq 0,\infty}} \xi_v(\pi_v)\right| \le 2\sqrt{q}.$$

在具有局部单值化元素 $\pi_v = T + a\,(a \in k^\times)$ 的位 v 处, 由 ξ 的定义可知

$$\begin{aligned}\xi_v(\pi_v) &= \xi_0(T+a)^{-1}\xi_\infty(T+a)^{-1}\\ &= \xi_0(a(1+a^{-1}T))^{-1}\xi_\infty(\pi_\infty^{-1}(1+a\pi_\infty))^{-1}\\ &= \chi(a)\psi(ca^{-1})\psi(ba).\end{aligned}$$

由此定理得证.

事实上, Deligne 在证明一般 Kloosterman 和的估计 (定理 8) 时也对分裂的情况进行了研究. 他有一个简单的方法可以从分裂情况导出非分裂情况也有同样的估计. 基于这一想法及 Mordell 的结果 (定理 10), Deligne[3] 猜测对扭曲的广义 Kloosterman 和应有同样的估计成立, 即

猜想(Deligne) 对 $N_n \times k_n$ 的非平凡特征标 (χ,ψ), 我们应有

$$\left|\sum_{x\in N_n} \chi(x)\psi(x)\right| \le nq^{\frac{n-1}{2}}.$$

推论 8 证实了上述猜想在 $n=2$ 时成立, 并且它也说明在 $n=2$ 时, 这一猜想可从有限域上曲线的 Riemann 猜想导出.

在本节的最后, 我们将给出另一个特征和的估计, 这一结论是首先由 N. Katz[5] 利用类似于 P. Deligne 采用的几何方法证明的. 我们在此给出的证明则是算术的. 它较 Katz 所用的方法要初等得多.

设 $F_1, F_2, \cdots, F_r$ 是有限域 k 的有限扩张, 其扩张次数之和是 n. 积 $F_1\times\cdots\times F_r$ 称为 k 上次数为 n **的平展代数** (étale algebra),

我们记作 B. 显然，域 k 可以对角地嵌入到 B 中. 对 B 中元素 $x=(x_1,\cdots,x_r)$, 如果有 $F_i=k(x_i)$, 并且 x_i 在 k 上的极小多项式是两两互素的 (也可称这些 x_i 是在 k 上两两不共扼的), 那么我们称 x 是**正则的** (reguler).

定理 11(Katz) 设 B 是 k 上次数为 n 的平展代数，x 是 B 的一个正则元素，则对 $B^\times$ 的任意非平凡特征标 χ, 有

$$\left|\sum_{\substack{a\in k\\ x-a\in B^\times}}\chi(x-a)\right|\le(n-1)\sqrt{q}.$$

证 记 $B=F_1\times F_2\times\cdots\times F_r$, $x=(x_1,\cdots,x_r)$, 以及 $\chi=(\chi_1,\cdots,\chi_r)$, 这里 χ_i 为 $F_i^\times$ 的特征标. 由于该特征和至多有 q 项，所以当 $n-1<\sqrt{q}$ 时, 该不等式是平凡的. 于是下面假定 $n-1<\sqrt{q}$, 则 $r\le n\le\sqrt{q}$. 以 $P_i(T)$ 表示 x_i 在 k 上的极小多项式，设 v_1, $\cdots$, v_r 是一些 $K=k(T)$ 的位，使得 P_i 为在 v_i 处的局部单值化元素. 则 $v_1,\cdots,v_r$ 和 ∞ 是 K 的不同的位，它们的剩余类域在映射 $T\longmapsto x_1,\cdots,x_r$ 和 $T^{-1}\longmapsto 0$ 下分别同构于 $F_1,\cdots,F_r$ 和 k. 对 $1\le i\le r$, 设 ω_{v_i} 是 $\mathcal{U}_{v_i}$ 的特征标，它在 $1+\mathfrak{p}_{v_i}$ 上平凡，并且在

$$\mathcal{U}_{v_i}/(1+\mathfrak{p}_{v_i})\cong F_i^\times$$

上它是由 χ_i^{-1} 给出的. 设 ω_∞ 是 $\mathcal{U}_\infty$ 的特征标，它在 $1+\mathfrak{p}_\infty$ 上平凡，在

$$\mathcal{U}_\infty/(1+\mathfrak{p}_\infty)\cong k^\times$$

上由 $\chi_i\cdots\chi_r$ 给出. 取 $\pi_\infty=1/T$, 定义 $\omega_\infty(\pi_\infty)=1$. 当位 $v\ne v_i,\cdots,v_r$ 和 ∞ 时，定义 ω_v 在 $\mathcal{U}_v$ 上平凡. 命 $\omega=\prod\limits_v\omega_v$, 显然它是 $\prod\limits_v\mathcal{U}_v\langle\pi_\infty\rangle$ 的一个特征标. 由于对 $a\in k^\times$,

$$\begin{aligned}\omega(a)&=\omega_{v_1}(a)\cdots\omega_{v_r}(a)\omega_\infty(a)\\&=\chi_1^{-1}(a)\cdots\chi_r^{-1}(a)(\chi_1\cdots\chi_r)(a)=1,\end{aligned}$$

故 ω 在 $k^\times$ 上平凡，因此 ω 可扩充为 $I_K/K^\times$ 上的一个伊代尔类特征标. 它是有限阶的，且由于至少有一个 $\chi_1,\cdots,\chi_r$ 是非平凡的，所以其前导子满足

$$0<\operatorname{cond}\omega\le v_1+\cdots+v_r+\infty.$$

设 Z 是 x 的那些位于 k 中的分量的全体. 于是，元素 $a\in k$ 要满足 $x-a\in B^\times$ 的充要条件是 $a\notin Z$. 在位 $v=a\in k-Z$ 处，我们可取 $\pi_v=T-a$, 于是

$$\begin{aligned}\omega_v(\pi_v)&=\omega_{v_1}(T-a)^{-1}\cdots\omega_{v_r}(T-a)^{-1}\omega_\infty(T-a)^{-1}\\&=\chi_1(x_1-a)\cdots\chi_r(x_r-a)\omega_\infty(\pi_\infty^{-1}(1-a\pi_\infty))^{-1}\\&=\chi(x-a).\end{aligned}$$

首先假定 ω 在所有位于 $Z\bigcup\{\infty\}$ 的位上分歧，则由推论 3 及 $\operatorname{cond}\omega$ 的次数 $\le\deg v_1+\cdots+\deg v_r+\deg\infty=n+1$ 知

$$\left|\sum_{\substack{\deg v=1\\ \omega_v:\ \text{非分歧}}}\omega_v(\pi_v)\right|=\left|\sum_{a\in k-Z}\chi(x-a)\right|\le(n-1)\sqrt{q}.$$

接下来，假定 ω 在 $Z\bigcup\{\infty\}$ 中的 j 个位处是非分歧的，则 $\deg(\operatorname{cond}\omega)\le n+1-j$. 从而由推论 3 得

$$\left|\sum_{\substack{\deg v=1\\ \omega_v:\ \text{非分歧}}}\omega_v(\pi_v)\right|\le(n-1-j)\sqrt{q}.$$

由此得到

$$\left|\sum_{a\in k-Z}\chi(x-a)\right|\le(n-j-1)\sqrt{q}+j\le(n-1)\sqrt{q}.$$

由此完成定理 11 之证明.

§4 一般形式的 Davenport-Hasse 等式

到目前为止，我们对伊代尔类特征标已有了比较多的了解，利用这些知识，我们给出在第一章 §5 中讨论过的 Davenport-Hasse 等式的另外一种解释. 首先简略地回顾一下 Davenport-Hasse 等式. 设 k 是一个有 q 个元素的有限域，取定 $k^\times$ 的一个非平凡乘法特征标 χ 和 k 的一个非平凡加法特征标 ψ, 由此定义 Gauss 和

$$g(\chi,\psi)=\sum_{\chi\in k^\times}\chi(x)\psi(x).$$

又设 k_n 是 k 的 n 次域扩张. $\mathrm{N}_{k_n/k}$ 和 $\mathrm{Tr}_{k_n/k}$ 分别为扩张 k_n/k 的范数映射和迹映射. Davenport-Hasse 等式给出了 Gauss 和 $g(\chi,\psi)$ 与 Gauss 和 $g(\chi\circ\mathrm{N}_{k_n/k},\psi\circ\mathrm{Tr}_{k_n/k})$ 之间的关系

$$(-g(\chi,\psi))^n=-g(\chi\circ\mathrm{N}_{k_n/k},\psi\circ\mathrm{Tr}_{k_n/k})$$

(参见第一章定理 6).

命 $K=k(T)$. 我们利用定理 10 的证明知道，存在 $I_K/K^\times$ 的一个伊代尔类特征标 ξ, 其导子为 $\mathrm{cond}\,\xi=1\cdot 0+2\cdot\infty$, 它在 $\mathcal{U}_0/1+\mathfrak{p}_0$ 上的限制 ξ_0 由 $\xi_0(x)=\chi(x)^{-1}$ 给出，而它在 $\mathcal{U}_\infty/1+\mathfrak{p}_\infty^2$ 上的限制 ξ_∞ 则由 $\xi_\infty(x(1+y\pi_\infty))=\chi(x)\overline{\psi}(y)$ 给出，这里 $\pi_\infty=1/T$, $x\in k^\times$ 和 $y\in k$. 我们已经证明了

$$\sum_{\substack{\deg v=1\\ v\neq 0,\infty}}\xi_v(\pi_v)=\sum_{x\in k^\times}\chi(x)\psi(x)=g(\chi,\psi).$$

由于 $\mathrm{cond}\,\xi$ 的次数为 3, 故可记 $L(s,\xi)=P(q^{-s},\xi)$. 从第五章定理 5 知， $P(u,\xi)$ 是一个次数为 1 的 u 的多项式. 于是从 $L(s,\xi)$

的定义得

$$P(u,\xi)=1+\sum_{\substack{\deg v=1\\ \xi_v:\text{非分歧}}}\xi_v(\pi_v)u=1+g(\chi,\psi)u.$$

设 E 是 K 与 k_n 的合成，即 $E=k_n(T)$. 特征标 ξ 与从 I_E 到 I_K 的范映射 $\mathrm{N}_{E/K}$ 之合成给出了 I_E 的一个伊代尔类特征标 $\xi\circ\mathrm{N}_{E/K}$. 同命题 1 所指出的那样，E 在 K 上是非分歧的. 从而对任意 K 的位 v 和任意能整除 v 的 E 的位 w, 局部范映射 N_{E_w/K_v} 映 U_w 为 U_v. 并且它还是个满射. 注意到在 E 的所有位中，能够整除 (K 的) 0 (或 ∞) 位的位只有一个，我们仍把它记作 0 (或 ∞). 由于 ξ 在 0 和 ∞ 外是非分歧的，于是 $\xi\circ\mathrm{N}_{E/K}$ 在 0 和 ∞ 外也是非歧的. 下面我们来讨论 $\xi_0\circ\mathrm{N}_{E_0/K_0}$ 和 $\xi_\infty\circ\mathrm{N}_{E_\infty/K_\infty}$. 由于 $\mathrm{N}_{E_0/K_0}(1+\mathfrak{p}_{0,E})=1+\mathfrak{p}_{0,E}$, 所以 $\xi_0\circ\mathrm{N}_{E_0/K_0}$ 在 $1+\mathfrak{p}_{0,E}$ 上平凡，在 $U_{0,E}/1+\mathfrak{p}_{0,K}\cong k_n^\times$ 上则满足

$$\xi_0\circ\mathrm{N}_{E_0/K_0}(x)=\xi_0(\mathrm{N}_{k_n/k}x)=\chi(\mathrm{N}_{k_n/k}x)^{-1}.$$

类似地，由

$$\mathrm{N}_{E_\infty/K_\infty}(1+\mathfrak{p}_{\infty,E}^2)=1+\mathfrak{p}_{\infty,K}^2$$

知，$\xi_\infty\circ\mathrm{N}_{E_\infty/K_\infty}$ 在 $1+\mathfrak{p}_{\infty,E}^2$ 上平凡，在 $U_{\infty,E}/1+\mathfrak{p}_{\infty,E}^2$ 上则满足：对任意的 $x\in k_n^\times$, $y\in k_n$, 有

$$\begin{aligned}&\xi_\infty\circ\mathrm{N}_{E_\infty/K_\infty}(x(1+y\pi_\infty))\\&=\xi_\infty((\mathrm{N}_{k_n/k}x)\mathrm{N}_{E_\infty/K_\infty}(1+y\pi_\infty))\\&=\xi_\infty((\mathrm{N}_{k_n/k}x)(1+(\mathrm{Tr}_{k_n/k}y)\pi_\infty))\\&=\chi(\mathrm{N}_{k_n/k}x)\overline{\psi}(\mathrm{Tr}_{k_n/k}y).\end{aligned}$$

用与前面同样的讨论可得

$$P(u,\xi\circ\mathrm{N}_{E/K})=1+g(\chi\circ\mathrm{N}_{k_n/k},\psi\circ\mathrm{Tr}_{k_n/k})u.$$

于是 Davenport-Hasse 等式可以改写为

$$P(u^n, \xi \circ \mathrm{N}_{E/K}) = \prod_{i=1}^{n} P(\zeta_n^i u, \xi),$$

其中 ζ_n 是一个 n 次本原单位根.

习题 4 验证在第一章 §5 中 Davenort-Hasse 等式的证明本质上就是上面的改写过程.

上面我们把 Hasse-Davenport 等式用一个关于 $P(u,\omega)$ 的等式表述出来, 其中 ω 是伊代尔类特征标, 这就为它的推广做好了准备. 下面域 K 将被允许为是常数域为 k 的任意单变量函数域. 对 $I_K/K^\times$ 的一个伊代尔特征标 ω, 从 §1 知, 它结合了一个 L-函数 $L(s,\omega)$, 该 L-函数是个有理函数, 其分子可以用 $P(q^{-s},\omega)$ 来表示. 其中 $P(u,\omega)$ 是一个关于 u 的多项式.

定理 12(Davenport-Hasse等式) *设 K 是常数域为 k 的单变量函数域, k_n 是 k 的 n 次扩张, $E = K \cdot k_n$. ω 是 $I_K/K^\times$ 的伊代尔类特征标. 则存在 I_K 的特征标 η, 它映 I_K^1 为 1, 映 I_K 中次数为 1 的伊代尔为 ξ_n, 且使得有下面等式成立*

$$L(s, \omega \circ \mathrm{N}_{E/K}) = \prod_{i=1}^{n} L(s, \eta^i \omega).$$

等价地, 我们有

$$P(u^n, \omega \circ \mathrm{N}_{E/K}) = \prod_{i=1}^{n} P(\zeta_n^i u, \omega).$$

证 利用命题 1 知, 扩张 E/K 是非分歧的. 又由推论 1, 对 K 的任意位 v 和任意可整除 v 的 E 的位 w, 局部范映射 N_{E_w/K_v} 映 U_w 为 U_v, 进而, $\omega \circ \mathrm{N}_{E/K}$ 只在这样一些位 w 处分歧, 这些 w 整除某个 K 上的 ω 分歧的位. 而在 E 的其他位处, $\omega \circ \mathrm{N}_{E/K}$ 是非分歧的. 设 v 是 K 上 ω 非分歧的一个位. 首先我们断言

$$\prod_{w|v} L(s, \omega_v \circ \mathrm{N}_{E_w/K_v}) = \prod_{i=1}^{n} L(s, \eta_v^i \omega_v).$$

以 κ_v 表示 K_v 的剩余类域. 同命题 1 一样, 命

$$d_v = [\kappa_v \bigcap k_n : k].$$

注意到 d_v 是 $\deg v$ 和 n 的最大公约数, 于是恰有 d_v 个 E 的位 w 整除 v, 且 $[E_w : K_v] = n/d_v$, 以及 $\deg w = (\deg v)/d_v$. 由于 E_w 在 K_v 上非分歧, 故可取 π_w 为 π_v, 从而

$$\begin{aligned}
&\prod_{w|v} L(s, \omega_v \circ \mathrm{N}_{E_w/K_v}) \\
&= \prod_{w|v} (1 - \omega_v(\pi_v)^{[E_w:K_v]}\ q^{-n(\deg w)s})^{-1} \\
&= (1 - \omega_v(\pi_v)^{n/d_v}\ q^{-sn\deg v/d_v})^{-d_v} \\
&= \prod_{i=1}^{n/d_v} (1 - \omega_v(\pi_v)\zeta_{n/d_v}^i\ q^{-s\deg v})^{-d_v} \\
&= \prod_{i=1}^{n} (1 - \omega_v(\pi_v)(\zeta_n^i q^{-s})^{\deg v})^{-1} \\
&= \prod_{i=1}^{n} (1 - \omega_v(\pi_v)\eta_v^i(\pi_v) q^{-s\deg v})^{-1} \\
&= \prod_{i=1}^{n} L(s, \eta_v^i \omega_v).
\end{aligned}$$

由此前述断言成立, 进而定理 12 的第一个结论成立. 当 ω 不是 $|\ |^{s_0} (s_0 \in \mathbf{C})$ 这种形式的特征标时, 第二个结论通过命 $u = q^{-s}$ 可以从第一个结论得出. 于是下面我们总假定 ω 在 I_K^1 上平凡, 且映每个次数为 1 的伊代尔为 a. 此时

$$L(s, \omega) = \frac{P(q^{-s}, \omega)}{(1 - aq^{-s})(1 - aq^{1-s})}.$$

于是

$$\prod_{i=1}^{n} L(s, \eta^i \omega) = \frac{\prod_{i=1}^{n} P(\zeta_n^i q^{-s}, \omega)}{(1 - a^n q^{-ns})(1 - a^n q^{n(1-s)})}.$$

另一方面，对 I_E 中任意次数为 1 的伊代尔 y, 我们由命题 1 知, $\mathrm{N}_{E/K}(y)$ 的次数是 n. 于是 $\omega \circ \mathrm{N}_{E/K}(y) = a^n$, 且

$$L(s, \omega \circ \mathrm{N}_{E/K}) = \frac{P(q^{-ns}, \omega \circ \mathrm{N}_{E/K})}{(1 - a^n q^{-ns})(1 - a^n q^{n(1-s)})}.$$

由此可以明显看出

$$\prod_{i=1}^{n} L(s, \eta^i \omega) = L(s, \omega \circ \mathrm{N}_{E/K})$$

等价于

$$\prod_{i=1}^{n} P(\zeta_n^i u, \omega) = P(u^n, \omega \circ \mathrm{N}_{E/K}).$$

于是定理得证.

Davenport-Hasse 等式还可以表述为下面更一般的形式，不过在此我们不证明它了.

定理 13 设 K 是一有理域上的单变量函数域，F 是 K 的有限 Abel 扩张，对 $I_K/K^\times$ 的任意伊代尔类特征标 ω, 我们有

$$L(s, \omega \circ \mathrm{N}_{F/K}) = \prod_{\eta} L(s, \eta\omega),$$

其中 η 跑遍 $I_K/K^\times \mathrm{N}_{F/K}(I_F)$ 的所有特征标.

习题 5 证明定理 12 为定理 13 的一种特殊情况.

注意 $\chi = \eta\omega$ 是 $I_K/K^\times$ 的一个满足

$$\chi \circ \mathrm{N}_{F/K} = \omega \circ \mathrm{N}_{F/K}$$

的特征标. 这就是说 χ 和 ω 提升出同一个 $I_F/F^\times$ 的特征标. 我们可以记 $I_F = \mathrm{GL}_1(A_F)$, 从而 $I_F/F^\times$ 的伊代尔类特征标可以看作是 $\mathrm{GL}_1(A_F)$ 上的 "自守形式". 映射 $\omega \longmapsto \omega \circ \mathrm{N}_{F/K}$ 就成为 $\mathrm{GL}_1(A_K)$ 上自守形式到 $\mathrm{GL}_1(A_F)$ 上自守形式的 "提升". 从自守形式的观点来看，定理 13 就是说，给出 $\mathrm{GL}_1(A_F)$ 的一个自守形式 ξ, 如果它可以由 $\mathrm{GL}_1(A_K)$ 中的自守形式 ω 提升得到，那么 ξ 的 L-函数恰是所有这样的 ω 的 L-函数之积. 更一般些，群 GL_1 可以用约化群

来代换，此时"提升映射"就被称为"基变换" (base change) 映射. 研究这种条件下的 Davenport-Hasse 等式是群表示论中一个非常困难的问题. 目前只是就 GL_n 的情况给出了答案：$n=1$ 是定理 13; $n=2$ 由 Langlands[6] 给出；一般的 n 是被 Arthur 和 Clozel[1] 所解决的. 关于自守形式和自守表示的基础知识我们将在第八章中予以介绍.

再回到定理 12, 命

$$P(u,\omega)=1+a_1u+\cdots+a_ru_r=(1-b_1u)\cdots(1-b_ru),$$

其中 $r=\deg P(u,\omega)$. 定理 12 指出，前导子 $\mathfrak{f}(\omega)$ 与 $\mathfrak{f}(\omega\circ\mathrm{N}_{E/K})$ 有相同的次数，于是我们可以记

$$\begin{aligned}P(u,\omega\circ\mathrm{N}_{E/K})&=1+A_1u+\cdots+A_ru^r\\&=(1-B_1u)\cdots(1-B_ru).\end{aligned}$$

必要时，将 $P(u,\omega\circ\mathrm{N}_{E/K})$ 的根的排到次序调整一下，从定理 12 可以看出，$B_i=b_i^n, i=1,2,\cdots,n$. 反过来，如果 $B_i=b_i^n, i=1,2,\cdots,n$, 那么我们有

$$P(u,\omega\circ\mathrm{N}_{E/K})=\prod_{i=1}^{n}P(\zeta_n^iu,\omega).$$

从而定理 12 等价于

定理 12′ 设 E 和 ω 均同定理 12, 则 $P(u,\omega\circ\mathrm{N}_{E/K})$ 的根是 $P(u,w)$ 的根的 n 次方.

在第五章中我们给出了关于 $L(s,w)$ 的函数方程，将它用 $P(u,\omega)$ 来表示得

$$P(u,\omega)=\varepsilon(\omega)u^rP\left(\frac{1}{qu},\omega^{-1}\right),$$

其中 $\varepsilon(\omega)$ 是一个常数，r 为 $P(u,\omega)$ 的次数. 即

$$r=\begin{cases}2g_k, & \text{若 } \omega=|\ |^{s_0},\ s_0\in\mathbf{C},\\ 2g_k-2+\deg\mathfrak{f}(\omega), & \text{其他情况}.\end{cases}$$

又因 $P(u,\omega^{-1})$ 的常数项为 1, 所以

$$\varepsilon(\omega) = a_r = (-1)^r b_1 \cdots b_r.$$

类似地

$$\varepsilon(\omega \circ \mathrm{N}_{E/K}) = A_r = (-1)^r B_1 \cdots B_r = (-1)^r (b_1 \cdots b_r)^n.$$

又由于 r 与 $\deg \mathfrak{f}(\omega) = \deg \mathfrak{f}(\omega \circ \mathrm{N}_{E/K})$ 有相同的奇偶性, 于是我们就得到了

推论 9 设 E 和 ω 同定理 12, 则

$$(-1)^{\deg \mathfrak{f}(\omega \circ \mathrm{N}_{E/K})} \varepsilon(\omega \circ \mathrm{N}_{E/K}) = ((-1)^{\deg \mathfrak{f}(\omega)} \varepsilon(\omega))^n.$$

当 ω 是本节开始时所述的 $I_K/K^\times$ 的伊代尔类特征标 ξ 时, 上面公式正好是 Davenport-Hasse 等式的原始形式.

§5 曲线的 zeta 函数

在第二章中, 我们研究了由方程 $a_0x_0^n + \cdots + a_rx_r^n = 0$ 所定义的射影簇的 zeta 函数, 在这一节中, 我们将利用 §2 和 §4 两节的结果来计算由

$$y_1^{n_1} = f_1(x), \quad \cdots, \quad y_r^{n_r} = f_r(x)$$

定义的仿射曲线 V 的 zeta 函数, 其中, $f_1, \cdots, f_r$ 是有限域 k 上的多项式. 为简单起见, 我们假定 $f_1, \cdots, f_r$ 只有单根, 并且它们是两两互素的. 同前面一样, 记 k 的势为 q, 同时假定 $n_1, \cdots, n_r$ 是 $q-1$ 的因子. 取定 $\widehat{k^\times}$ 的生成元 χ. 以 N_n 表示 v 在 k_n 上点的个数, 利用 §2 后面部分的讨论知

$$N_1 = q + \sum_{x \in k} \sum_{\substack{0 \le j_i \le n_i - 1 \\ j_i \text{不全为} 0}} \chi(f_1^{j_1 e_1}(x) \cdots f_r^{j_r e_r}(x)),$$

其中 $e_i = (q-1)/n_i$, $i = 1, 2, \cdots, r$. 由于有 $n_i | q-1$ 的假定, 所以在计算 N_n 时, 只需在 N_1 的表达式中把 q 换成 q^n, 把 χ 换成

$\chi \circ \mathrm{N}_{k_n/k}$ 即可，即

$$N_n = q^n + \sum_{x \in k_n} \sum_{\substack{0 \le j_i \le n_i - 1 \\ j_i \text{ 不全为 } 0}} \chi \circ \mathrm{N}_{k_n/k}(f_1^{j_1 e_r}(x) \cdots f_r^{j_r e_r}(x)).$$

因此

$$\sum_{n=1}^{\infty} N_n u^{n-1} = \sum_{n=1}^{\infty} q^n u^{n-1} + \sum_{\substack{0 \le j_i \le n_i - 1 \\ j_i \text{ 不全为 } 0}} \sum_{n=1}^{\infty} \sum_{x \in k_n} (\chi \circ \mathrm{N}_{k_n/k}(f_1^{j_1 e_1}(x) \cdots f_r^{j_r e_r}(x)) u^{n-1}).$$

固定一个 r 元组 $J = (j_1, \cdots, j_r)$，其中 $0 \le j_i \le n_i - 1$ 且存在 $j_i \neq 0$. 我们先对 n 求和. 由 $f_1, \cdots, f_r$ 的假定知

$$f^J(x) = f_1^{j_1 e_1}(x) \cdots f_r^{j_r e_r}(x)$$

是一个多项式，并且 $f^J(x)$ 不是另一个 k 上的多项式的 $q-1$ 次幂. 设 $K = k(T)$ 是 k 上的有理函数域，以 ω_J 表示按定理 4 证明中所述方法用 χ 和 f^J 构造出的 $I_K/K^\times$ 的伊代尔类特征标. 则 ω_J 并非处处非分歧，并且

$$\sum_{\substack{v \in \mathrm{Supp}\, f^J \\ v \neq \infty}} v \le \mathrm{cond}\, \omega_J \le \sum_{v \in \mathrm{Supp}\, f^J} v,$$

以及

$$P(u, \omega_J) = 1 + a_1 u + \cdots + a_r u^r = (1 - b_1 u) \cdots (1 - b_r u).$$

同时还有

$$\sum_{x \in k} \chi(f^J(x)) = \begin{cases} a_1, & \text{若 } \omega_J \text{ 在 } \infty \text{ 处分歧}, \\ a_1 - 1, & \text{若 } \omega_J \text{ 在 } \infty \text{ 处非分歧}. \end{cases}$$

类似地，若 $E_n = K \cdot k_n$，设

$$P(u, \omega_J \circ \mathrm{N}_{E_n/K}) = 1 + A_1 u + \cdots + A_r u^r,$$

则利用上节的讨论得

$$\sum_{x\in k_n}\chi\circ \mathrm{N}_{k_n/k}(f^J(x))=\begin{cases}A_1, & 若\ \omega_J\ 在\infty\ 处分歧,\\ A_1-1, & 若\ \omega_J\ 在\infty\ 处非分歧.\end{cases}$$

另一方面，利用定理 12′ 得

$$a_1=-b_1-\cdots-b_r,\qquad A_1=-b_1^n-\cdots-b_r^n.$$

综合这些讨论，当 $|u|$ 足够小时，我们有

$$\begin{aligned}&\sum_{i=1}^{\infty}\sum_{x\in k_n}\chi\circ \mathrm{N}_{k_n/k}(f^J(x))u^{n-1}\\ &=-\frac{b_1}{1-b_1u}-\cdots-\frac{b_r}{1-b_ru}\\ &\quad-\begin{cases}0, & 若\ \omega_J\ 在\infty\ 处分歧\\ 1/(1-u), & 若\ \omega_J\ 在\infty\ 处非分歧\end{cases}\\ &=\frac{P'(u,\omega_J)}{P(u,\omega_J)}-\begin{cases}0, & 若\ \omega_J\ 在\infty\ 处分歧,\\ 1/(1-u), & 若\ \omega_J\ 在\infty\ 处非分歧.\end{cases}\end{aligned}$$

从而存在整数 $m\geq 0$，使得

$$\sum_{n=1}^{\infty}N_nu^{n-1}=\frac{q}{1-qu}+\sum_J\frac{P'(u,\omega_J)}{P(u,\omega_J)}-\frac{m}{1-u}.$$

我们把定义 V 的联立方程齐性化，若它们定义了一条 k 上的非奇异曲线 $\overline{V}$，则在加上无穷远处点的个数后，我们得到

$$\frac{Z'_{\overline{V}}(u)}{Z_{\overline{V}}(u)}=\sum_{n=1}^{\infty}\overline{N}_nu^{n-1}=\frac{q}{1-qu}+\frac{1}{1-u}+\sum_J\frac{P'(u,\omega_J)}{P(u,\omega_J)}.$$

由于只有非平凡的 $P(u,\omega_J)$ 才有绝对值为 $q^{-1/2}$ 的根，从而根据非奇异射影簇的 zeta 函数的一般形式，我们可以看出，$\overline{V}$ 的 zeta 函数应该是

$$Z_{\overline{V}}(u)=\frac{\prod\limits_J P(u,\omega_J)}{(1-u)(1-qu)}.$$

接下来，我们就一个具体的情况作为例子来加以讨论. 设 $\gamma, \delta \in k^{\times}$, a, b 均与 q 互素， q 为有限域 k 的势. 设 V 是由 $y^b = \gamma x^a + \delta$ 定义的平面曲线. 注意 $f(x) = \gamma x^a + \delta$ 只有单根. 进一步假定 a 与 b 互素， b 整除 $q - 1$. 设 χ 是 $k^{\times}$ 的一个阶为 b 的特征标. 由上面的讨论看出，仿射曲线 V 在 k_n 上点的个数 N_n 等于

$$N_n = q^n + \sum_{x \in k_n} \sum_{j=1}^{b-1} \chi \circ \mathrm{N}_{k_n/k}\ (f(x))^j.$$

设 $K = k(T)$, ω^j 是由 χ^j 和 $f(x)$ 按 §2 中所述方法构造出的 $I_K/K^{\times}$ 的伊代尔类特征标，由于 $\deg f = a$ 与 χ^j 的阶互素，所以 ω^j 的前导子 $\mathrm{cond}\ \omega^j$ 的阶等于 $a + 1$. 因此 $P(u, \omega^j)$ 是一个次数为 $a - 1$ 的 u 的多项式，而射影簇 $\overline{V}$ 的 zeta 函数是

$$Z_{\overline{V}}(u) = \frac{P(u, \omega) \cdots P(u, \omega^{b-1})}{(1 - u)\ (1 - qu)}.$$

另一方面， $\gamma x^a - y^b + \delta = 0$ 在 k_n 中解的个数 N_n 已在第二章 §1 中计算过. 利用那里的方法，首先将方程改写为

$$\delta^{-1} \gamma x^a - \delta^{-1} y^b + 1 = 0.$$

命 $d_0 = (a, q^n - 1)$, $d_1 = (b, q^n - 1) = b$, 则

$$\begin{aligned} N_n =& q^n + \sum \chi_0(\delta\gamma^{-1})\chi_1(-\delta) j(\chi_1, \chi_2) \\ & - \sum \chi_0(\delta r^{-1})\chi_1(-\delta) j(\chi_1), \end{aligned}$$

其中两个和式分别是对 $k_n^{\times}$ 的特征标 χ_0, χ_1, χ_2 与 χ_0, χ_1 求和，它们均要求 $\chi_0^{d_0} = \chi_1^b = 1$, 不过第一个和式还要求 $\chi_0, \chi_1, \chi_2 \neq 1$ 且 $\chi_0\chi_1\chi_2 = 1$; 而第二个和式则要求 $\chi_0, \chi_1 \neq 1$ 且 $\chi_0\chi_1 = 1$. 由于我们假定了 a 与 b 互素，于是 d_0 与 b 互素，从而第二个求和范围是空集.

我们现在可以按第二章 §2 中方法来计算 $\overline{V}$ 的 zeta 函数. 我

们有

$$Z_{\overline{V}} = \frac{\prod\limits_{(\chi_0,\chi_1,\chi_2)} \left(1 - c(\chi_0,\chi_1,\chi_2)u^{\mu(\chi_0,\chi_1,\chi_2)}\right)}{(1-u)\ (1-qu)}.$$

其中

$$c(\chi_0,\chi_1,\chi_2) = \chi_0(\delta\gamma^{-1})\chi_1(-\delta)j(\chi_1,\chi_2),$$

乘积要求 χ_0,χ_1,χ_2 是 k 的一个 $\mu=\mu(\chi_0,\chi_1,\chi_2)$ 次扩张 k_μ 的乘法特征标，并且 $\chi_0^{d_0}=1$, $\chi_1^b=1$, χ_0, χ_1, $\chi_2 \neq 1$, $\chi_0\chi_1\chi_2=1$. 此外，还要求不存在 k_μ 的任何真子域 k_m，使得 χ_0, χ_1, χ_2 可以由 $k_m^\times$ 的特征标复合范映射 N_{k_μ/k_m} 而得到. 可以看出在每个 Galois 轨道中只能选出一个这样的三元组.

下面就 V 是由方程 $y^2=\gamma x^3+\delta=f(x)$ 定义的椭圆曲线这种特殊情况来比较 $Z_{\overline{V}}(u)$ 的两种表述，不过在这里我们还要求 char $k\neq 2,3$. 此时 $Z_{\overline{V}}(u)$ 的分子为

$$P(u,\omega) = 1 + \sum_{x\in k}\chi(f(x))u + qu^2,$$

其中 χ 是 $k^\times$ 的二次特征标. 接下来我们分两种情况来研究第二个表达式.

情形 1： $q\equiv 1(\mathrm{mod}\,3)$. 此时 $\gcd(3,q-1)=3$. 设 χ_0 是 $k^\times$ 的一个 3 阶特征标. $k^\times$ 的另一个 3 阶特征标为 $\overline{\chi}_0$. 同前面一样，设 χ 是 $k^\times$ 的二次特征标，则

$$\begin{aligned}P(u,\omega) = &(1-\chi_0(\gamma^{-1}\delta)\chi(-\delta)j(\chi,\chi\overline{\chi}_0)u)\\ &\times(1-\overline{\chi}_0(\gamma^{-1}\delta)\chi(-\delta)j(\chi,\chi\chi_0)u).\end{aligned}$$

情形 2： $q\equiv 2(\bmod\ 3)$. 此时 $\gcd(3,q-1)=1$，以及 $\gcd(3,q^2-1)=3$. 设 χ_0 是 $k_2^\times$ 的一个 3 阶特征标. $Z_{\overline{V}}(u)$ 的第二种表达式中含有 χ_0 的项只有一个，在此项上，

$$\chi_1=\chi\circ\mathrm{N}_{k_2/k},\quad \chi_2=\chi_0^{-1}\chi_1,\quad \mu(\chi_0,\chi_1,\chi_2)=2.$$

于是

$$P(u,\omega) = 1 + \sum_{x \in k} \chi(f(x))u + qu^2 = 1 - c(\chi_0, \chi_1, \chi_2)u^2.$$

由此看出

$$\sum_{x \in k} \chi(f(x)) = 0,$$

以及

$$c(\chi_0, \chi_1, \chi_2) = -q.$$

从几何上看， $\overline{V}$ 是 P^1 的一个有限覆盖. 若我们把这个覆盖映射取为 $(x,y) \longmapsto x$, 则我们取 P^1 的函数域为 $K = k(x)$. $\overline{V}$ 的函数域为 $k(x,y) = F$, 且使得 F 是 K 的二次 Galois 扩张. 因此 $K^\times \mathrm{N}_{F/K}(I_F)$ 是 I_K 的一个二阶开子群, 伊代尔类特征标 ω 在 $I_K/K^\times$ 上是非平凡的, 且

$$\zeta_F(s) = L(s,\omega)\zeta_K(s).$$

如果我们把覆盖映射取为 $(x,y) \longmapsto y$. 则 $\mathbf{P}^1$ 的函数域应取为 $K = k(y)$, $\overline{V}$ 的函数域为 $k(x,y) = F$. 当 $q \equiv 2 \pmod 3$ 时， F 在 K 上是非 Galois 的. 但当 $q \equiv 1 \pmod 3$ 时， F/K 是 Galois 的, 其 Galois 群是个 3 阶循环群. 从类域论可知, 存在 $I_K/K^\times \mathrm{N}_{F/K}(I_F)$ 的两个 3 阶伊代尔类特征标 ξ 和 $\overline{\xi}$, 使得

$$\zeta_F(s) = L(s,\xi)L(s,\overline{\xi})\zeta_K(s).$$

特征标 ξ 和 $\overline{\xi}$ 是什么呢？由情形 1 的讨论可知, 它们的 P 函数是

$$1 - \chi_0(\gamma^{-1}\delta)\chi(-\delta)j(\chi, \chi\overline{\chi}_0)u$$

和

$$1 - \overline{\chi}_0(\gamma^{-1}\delta)\chi(-\delta)j(\chi, \chi\chi_0)u.$$

为了更精确一些, 借助曲线定义的方程 $y^2 = \gamma x^3 + \delta$, 即 $x^3 = h(y)$, 其中 $h(y) = \gamma^{-1}y^2 - \gamma^{-1}\delta$. 由于 χ_0 为 $k^\times$ 的 3 阶特征标, 所以利

用 χ_0 和 h 我们可以构造出 $I_K/K^\times$ 的一个伊代尔类特征标 ξ, 它在 ∞ 处分歧, 且 $\mathrm{cond}\,\xi$ 的次数是 3. 从而 $P(u,\xi)$ 次数为 1. 我们同样可以证明

$$Z_{\overline{V}}(u) = \frac{P(u,\xi)P(u,\overline{\xi})}{(1-u)(1-qu)} = \frac{P(u,\omega)}{(1-u)(1-qu)}.$$

于是 $P(u,\xi)$ 是 $P(u,\omega)$ 的一个因子, 进而 ξ 和 $\overline{\xi}$ 就是我们所要的特征标.

习题 6 设 V 是由 $y^b = \gamma x^a + \delta$ 定义的曲线, 其中 $\gamma, \delta \in k^\times$, a 和 b 是不能被 $\mathrm{char}\,k$ 整除的互素整数, 且 $b \mid q-1$. 设 χ 是 $k^\times$ 的阶为 b 的特征标, $K = k(T)$. 又设 ω^i 是由 χ^i 和 $f(x) = \gamma x^a + \delta$ 构造的 $I_K/K^\times$ 的伊代尔类特征标. 证明: 在 $Z_{\overline{V}}(u)$ 的两种表达式中, 其分子表达式之间有下面的关系

$$P(u,\omega^i) = \prod_{\chi_0}(1 - c(\chi_0, \chi^i, \overline{\chi}_0\overline{\chi}^i)u^{\mu(\chi_0,\chi^i,\overline{\chi}_0\overline{\chi}^i)}),$$

其中 χ_0 跑遍 $k_n^\times$ 上阶可整除 $\gcd(a, q^\mu - 1)$ 的非平凡特征标的 Galois 轨道全体.

参 考 文 献

[1] J. Arthur and L. Clozel, *Simple Algebras, Base Change, and the Advanced Theorey of the Trace Formula*, Annals of Math. Studies 120 Princeton Univ. Press, Princeton, New Jersey 1989.

[2] J. W. S. Cassels and A. Fröhlich, *Algebraic Number Theory*, Thompson, Washington 1967, republished by Academic Press, London, 1989.

[3] P. Deligne, *Cohomologie étale* (SGA $4\frac{1}{2}$), Lecture Notes in Math., 569, Springer-Verlag, Berlin, Heidelberg, New York, 1977.

[4] N. Jacobson, *Basic Algebra I*, Freeman, San Francisco 1980 (中译本: 《基础代数》, 一卷一、二分册, 高教出版社, 北京, 1988).

[5] N. Katz, *An estimate for character sums*, J. Amer. Math. Soc., **2** (1989), 197~200.

[6] R. Langlands, *Base Change for GL_2*, Annals of Math. Studies, 96, Princeton Univ. Press, Princeton, New Jersey, 1980.

[7] S. Lang , *Algebraic Number Theory*, Springer-Verlag, New York, Berlin, Heidelberg, 1986.

[8] W.-C. W. Li(李文卿), *Character sums and abelian Ramanujan graphs*, J. of Number Theory **41** (1992), 199~217.

[9] W. Schmidt, *Equations over Finite Fields,* Lecture Notes Notes in Math., 536, Springer-Verlag, Berlin, Heidelberg, New York, 1976.

[10] A. Weil, *On some exponential sums*, Proc. National Academy of Science, **34** (1948), 204~207.

[11] A. Weil, *Basic Number Theory*, Springer-Verlag, Berlin, Hiedelberg, New York, 1973.

第七章　模形式理论

在这一章中，我们将概述经典模形式理论的基本概念和结果.

§1　模　形　式

所谓 Poincaré 上半平面 $\mathfrak{H}$ 是指复平面 $\mathbf{C}$ 的上半平面，即集合 $\{z \in \mathbf{C} : \mathrm{Im}(z) > 0\}$.

令 Γ 表示矩阵群

$$\mathrm{SL}_2(\mathbf{Z}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in \mathbf{Z}, ad - bc = 1 \right\}.$$

它以线性变换的方式作用在 Poincaré 上半平面 $\mathfrak{H}$ 上，即对

$$\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma, \quad xz \in \mathfrak{H},$$

有

$$\gamma z = \frac{az + b}{cz + d}.$$

习题 1　设 γ, z 同上，证明

$$\mathrm{Im}(\gamma z) = \frac{\mathrm{Im}(z)}{|cz + d|^2}.$$

这个习题表明 $\mathfrak{H}$ 在 Γ 作用下仍旧是 $\mathfrak{H}$. 轨道空间 $\mathfrak{H}/\Gamma$ 常常用一个区域来表示，该区域称为 Γ 的**基本区域**, 通常取作 $\mathcal{D}$, 如下页图 3 所示. 注意，在此图中，点 $-1/2 + \mathrm{i}y$ 与点 $1/2 + \mathrm{i}y$ $(y > 0)$, 点 $\mathrm{e}^{\mathrm{i}\theta}$ 与点 $\mathrm{e}^{\mathrm{i}(\pi - \theta)}$ $(\pi/3 \le \theta \le \pi/2)$ 均在同一轨道上.

给出 $\mathfrak{H}$ 上双曲度量 $y^{-2}\mathrm{d}x\mathrm{d}y$, 当 y 趋于 $+\infty$ 时，点 $-1/2 + \mathrm{i}y$ 与点 $1/2 + \mathrm{i}y$ 间的距离是趋于 0 的. 于是区域 $\mathcal{D}$ 看上去就像是一

个有孔的球面. 点 $i\infty$ 称为 Γ 的**尖点**, $i\infty$ 在 Γ 下的轨道是由 $i\infty$ 与实轴上的有理点构成, 它们也都称为 Γ 的**尖点**.

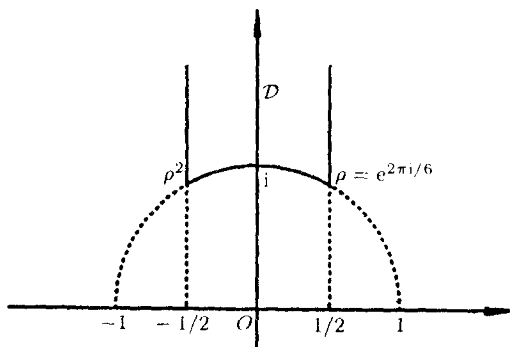


图 3

注 $\mathcal{D}$ 中的点可以参数化 $\mathbf{C}$ 上的椭圆曲线. 事实上, 一条 $\mathbf{C}$ 上的椭圆曲线总可以写成 $\mathbf{C}/L$ 的形式, 其中 L 是 $\mathbf{C}$ 上的一个格, 即 $\mathbf{C}$ 中秩为 2 的 $\mathbf{Z}$ 模. 如果存在一个从椭圆曲线 $\mathbf{C}/L$ 到椭圆曲线 $\mathbf{C}/L'$ 的解析群同构 f, 我们称这两条椭圆曲线是**等价的**. 此时, 对任意的 $z, z_1 \in \mathbf{C}$, 有

$$f(z+z_1) = f(z) + f(z_1).$$

固定 z_1, 仅以 z 为变量, 对上式两边微分得 $f'(z+z_1) = f'(z)$. 由 z_1 的任意性知, $f'(z) = u$ 是个常数, 又因 $f(0)=0$ 且 f 为单射, 所以我们可以断言, $f(z) = uz$, 其中 u 为非零常数. 换句话说, $\mathbf{C}/L$ 与 $\mathbf{C}/L'$ 等价的充要条件是: 存在 $u \in \mathbf{C}^\times$, 使得 $uL = L'$. 此时我们称这两个格是**等价的**. 在给定的一个格的等价类中, 我们总可找到一个格, 它的基是 $\{z, 1\}$, 其中 $z \in \mathfrak{H}$. 而两个具有基 $\{z,1\}$ 和 $\{z',1\}$ 的格等价的充要条件是: z 和 z' 位于 $\mathfrak{H}$ 中同一条 Γ 轨道中. 因此 $\mathfrak{H}/\Gamma$ 参数化了 $\mathbf{C}$ 上的椭圆曲线等价类.

习题 2 (1) 将 $\mathrm{d}x \wedge \mathrm{d}y$ 表成 $\mathrm{d}z \wedge \mathrm{d}\bar{z}$ 的形式;

(2) 证明度量 $y^{-2}\mathrm{d}x\mathrm{d}y$ 是 Γ 不变的.

习题 3 (1) 证明格 $L(z)=\mathbf{Z}z+\mathbf{Z}\cdot 1$ 与格 $L(z')=\mathbf{Z}z'+\mathbf{Z}\cdot 1$ 等价的充要条件是：存在 $\gamma\in\Gamma=\mathrm{SL}_2(\mathbf{Z})$, 使得 $z'=\gamma z$;

(2) 当 $z'=\gamma z$ 时，描述由 $\mathbf{C}/L(z)$ 到 $\mathbf{C}/L(z')$ 的同构.

设 H 是 Γ 的一个有限阶子群，则 H 的基本区域是由有限多个 Γ 的基本区域并起来的，它有有限多个尖点，这些尖点均在 Γ 尖点的 H 轨道中. $\mathfrak{H}/H$ 的紧致化，记作 $\widehat{\mathfrak{H}/H}$, 是一个亏格为 g 的 Riemann 面，即 $\mathbf{C}$ 上一条亏格为 g 的曲线. 关于 Riemann 面 $\widehat{\mathfrak{H}/H}$ 的亏格 g 的计算，请读者参阅参考文献 [9].

习题 4 设 H 为 Γ 的一个有限阶子群，则存在 $a_0,a_1,\cdots,a_r\in\Gamma$, 有下面不交陪集表示：

$$\Gamma=a_0H\bigcup a_1H\bigcup\cdots\bigcup a_rH.$$

证明 H 的基本区域 $\mathcal{D}(H)$ 可以取作

$$\mathcal{D}(H)=a_0\mathcal{D}\bigcup a_1\mathcal{D}\bigcup\cdots\bigcup a_r\mathcal{D}.$$

习题 5 求 Riemann 面 $\widehat{\mathfrak{H}/\Gamma}$ 的亏格.

习题 6 设 $c_1,\cdots,c_s$ 为 H 的尖点，证明轨道 $Hc_1,\cdots,Hc_s$ 中点集的并恰为 $\{i\infty\}\bigcup\mathbf{Q}$.

定义在 $\mathfrak{H}/H$ 上的全纯微分总可以写成 $f(z)\mathrm{d}z$ 的形式，其中 $f(z)$ 是 $\mathfrak{H}$ 上的全纯函数，且满足关系

$$f(\gamma z)\mathrm{d}(\gamma z)=f(z)\mathrm{d}z,\quad y\gamma\in H.$$

类似地，若 $f(z)\mathrm{d}z^k$ 是一个全纯 k-微分，则 f 是 $\mathfrak{H}$ 上满足关系

$$f(z)=(cz+d)^{-2k}f(\gamma z),\qquad \gamma=\begin{pmatrix}a & b\\ c & d\end{pmatrix}\in H$$

的全纯函数. 一般地，对正整数 k, 定义"划算子"(记为 $|_k$) 如下：

$$(f\mid_k\gamma)(z)=(\det\gamma)^{k/2}(cz+d)^{-k}f(\gamma z),$$

其中

$$\gamma=\begin{pmatrix}a & b\\ c & d\end{pmatrix}\in\mathrm{GL}_2^+(R)$$

(具有正行列式之值的二阶可逆实矩阵群). 于是, 对任意正数 x, 我们有

$$\left(f|_k \begin{pmatrix} x & 0 \\ 0 & x \end{pmatrix}\right)(z) = f(z).$$

设 H 为 Γ 的有限阶子群, f 是定义在 $\mathfrak{H}$ 上的函数, 如果 f 满足:

(1) f 在 $\mathfrak{H}$ 上全纯;

(2) $(f|_k \gamma)(z) = f(z), \quad \gamma \in H$;

(3) f 在 H 的所有尖点处全纯;

则称 f 为 H 上的一个权为 k 的**模形式**.

条件 (1) 和 (2) 是很容易理解的. 现在我们解释一下条件 (3). 由于 H 在 Γ 中的指数有限,所以它一定包含一些平移变换 $\begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix}$, 其中 $m \neq 0$. 设 M 是使 $\begin{pmatrix} 1 & M \\ 0 & 1 \end{pmatrix} \in H$ 成立的最小正整数, 由条件 (2) 可知, $f(z) = f(z+M)$, 于是 f 有一个 Fourier 展开

$$f(z) = \sum_{n=-\infty}^{\infty} a_n \mathrm{e}^{2\pi \mathrm{i} n z/M}.$$

由于 $\mathrm{e}^{2\pi \mathrm{i} n z/M}$ 是在 $\mathrm{i}\infty$ 处的局部单值化参数, 于是在 $\mathrm{i}\infty$ 处全纯是指上述展式是一个关于 $\mathrm{e}^{2\pi \mathrm{i} z/M}$ 的 Taylor 展式, 即, 当 $n < 0$ 时, $a_n = 0$. 对于任意的 $\gamma \in \Gamma$, 如果 $f|_k \gamma^{-1}$ 在 $\mathrm{i}\infty$ 处全纯, 我们则称 **f 在尖点 $\gamma(\mathrm{i}\infty)$处全纯**.

H 上权 k 的模形式全体构成了一个线性空间, 记作 $\mathcal{M}(H,k)$.

一个模形式如果在所有的尖点处为 0, 则我们称它为**尖点形式**. H 上的尖点形式全体构成了 $\mathcal{M}(H,k)$ 的一个子空间 $C(H,k)$. 要提醒读者的是, $C(H,2)$ 恰好由那些在 $\mathfrak{H}$ 上定义、且满足 $f(z)\mathrm{d}z$ 是 $\widehat{\mathfrak{H}/H}$ 上全纯微分的函数 f 组成. 事实上, 在尖点 $\mathrm{i}\infty$ 处, 设 $q = \mathrm{e}^{2\pi \mathrm{i} z/M}$ 为其局部单值化参数. 由于

$$\mathrm{d}q = \frac{2\pi \mathrm{i}}{M} q \mathrm{d}z,$$

所以

$$f(z)\mathrm{d}z = f(q)\frac{2\pi\mathrm{i}}{M}\frac{1}{q}\mathrm{d}q.$$

于是 $f(z)\mathrm{d}z$ 在 $\mathrm{i}\infty$ 处全纯的充分必要条件是 f 在 $\mathrm{i}\infty$ 处为 0. 同样的讨论也适用于其他尖点. 这也说明 $\dim \mathcal{C}(H,2)$ 等于 $\widehat{\mathfrak{H}/H}$ 的亏格. 我们也称它为**群 H 的亏格**.

习题 7 若 k 是一个奇数, 证明 $\mathcal{M}(\Gamma,k)=\{0\}$.

研究最多的 Γ 的子群是下面三类所谓的同余子群:

$$\Gamma(N)=\left\{\gamma\in\Gamma:\gamma\equiv\begin{pmatrix}1&0\\0&1\end{pmatrix}\bmod N\right\}\lhd\Gamma,$$

$$\Gamma_1(N)=\left\{\gamma\in\Gamma:\gamma\equiv\begin{pmatrix}1&*\\0&1\end{pmatrix}\bmod N\right\}$$

和

$$\Gamma_0(N)=\left\{\gamma\in\Gamma:\gamma\equiv\begin{pmatrix}*&*\\0&*\end{pmatrix}\ \bmod N\right\}.$$

事实上, Γ 的任意子群如果包含了某个 $\Gamma(N)$, 那么我们都称它是**同余子群** ($\Gamma(N)$ 亦称为**主同余子群**). 但在本书中, 我们主要考虑上述三类子群. 类似于 $\mathfrak{H}/\Gamma$, 模曲线 $\mathfrak{H}/\Gamma(N)$, $\mathfrak{H}/\Gamma_1(N)$ 和 $\mathfrak{H}/\Gamma_0(N)$ 将具有下面类型加法结构的椭圆曲线按一定的等价关系予以分类.

我们知道, 椭圆曲线 $E=\mathbf{C}/L$ 的阶可以整除 N 的点的全体构成了群

$$E(N)=\frac{1}{N}L/L\cong\mathbf{Z}/N\mathbf{Z}\times\mathbf{Z}/N\mathbf{Z}.$$

因此 E 可以有三种加法结构. 首先我们在 E 上选取两个 N 阶点 P 和 Q, 使得作为 $\mathbf{Z}/N\mathbf{Z}$ 模, $E(N)$ 由 P 和 Q 生成. 两个这样的椭圆曲线等价意味着存在一个从 E 到 E' 的同构, 它映 P 为 P', Q 为 Q'. 我们用三元组 $(E;P,Q)$ 来代表这样的椭圆曲线; 类似的, 我们用 $(E;P)$ 来代表这样一种的椭圆曲线, 我们在它上面取一个 N 阶点 P, 使得任意两条 $(E;P)$ 和 $(E';P')$ 这样的椭圆曲线, 若它们等价, 则在它们之间存在一个映 P 到 P' 的同构; $(E;C)$ 则

表示在 $E(N)$ 中取定一个 N 阶循环群 C 的椭圆曲线 E, 并且若两条 (E,C) 和 (E',C') 这样的椭圆曲线等价的话，则有一个映 C 为 C' 的同构. 对 $\mathfrak{H}$ 上点 z, 我们用 $L(z)$ 表示格 $\mathbf{Z}z+\mathbf{Z}\cdot 1$. 记 $E(z)$ 为椭圆曲线 $\mathbf{C}/L(z)$,

$$P(z)=\frac{1}{N}\in E(z),\quad Q(z)=\frac{1}{N}z\in E(z),$$

而 $C(z)$ 则表示由 $1/N$ 生成的 $E(z)$ 中的循环群.

定理 1 (1) 椭圆曲线 $(E;P,Q)$ 总与某个 $(E(z);P(z),Q(z))$ 等价，这里 $z\in\mathfrak{H}$, 并且曲线 $(E(z);P(z),Q(z))$ 同 $(E(z');P(z'),Q(z'))$ 等价的充要条件是：存在 $\gamma\in\Gamma(N)$, 使得 $z'=\gamma(z)$. 于是 $\mathfrak{H}/\Gamma(N)$ 将 $(E;P,Q)$ 这样的椭圆曲线按此等价关系予以分类.

(2) 椭圆曲线 $(E;P)$ 的等价类也可以用某个 $(E(z);P(z))$ 来代表，其中 $z\in\mathfrak{H}$. 而且，曲线 $(E(z);P(z))$ 同 $(E(z');P(z'))$ 等价的充要条件是，存在 $\gamma\in\Gamma_1(N)$, 使得 $z'=\gamma(z)$. 于是 $\mathfrak{H}/\Gamma_1(N)$ 将 $(E;P)$ 这样的椭圆曲线按此等价关系予以分类.

(3) 椭圆曲线 $(E;C)$ 的等价类同样可以用某个 $(E(z);C(z))$ 来代表，其中 $z\in\mathfrak{H}$. 而且，曲线 $(E(z);C(z))$ 同 $(E(z');C(z'))$ 等价的充要条件是，存在 $\gamma\in\Gamma_0(N)$, 使得 $z'=\gamma(z)$. 于是 $\mathfrak{H}/\Gamma_0(N)$ 将 $(E;C)$ 这样的椭圆曲线按此等价关系予以分类.

证 给定椭圆曲线 $(E;P,Q)$, 其中 $E=\mathbf{C}/L$, P 和 Q 可以分别用两个复数 p 和 q 来表示. 由于 P 和 Q 是 $\mathbf{Z}$ 线性无关的，所以 q/p 是一个复数. 如果必要，给 q 添加一个合适的格点，我们总能假定 $\mathrm{Im}\,(q/p)>0$. 这即是说 $z=(q/p)\in\mathfrak{H}$. 由于 NP 和 NQ 生成格 L, 所以乘以 $1/Np$ 运算给出了一个从 $\mathbf{C}/L$ 到 $\mathbf{C}/L(z)$ 的同构，且映 P 为 $P(z)=1/N$, Q 为 $Q(z)=z/N$. 这就证明了 (1), (2) 和 (3) 中的第一部分论述.

下面设乘以非零复数 u 的运算分别为在 (1), (2) 或 (3) 中由椭圆曲线 $(E(z);P(z),Q(z))$, $(E(z);P(z))$ 或 $(E(z);C(z))$ 到 $(E(z');P(z'),Q(z'))$, $(E(z');P(z'))$ 或 $(E(z');C(z'))$ 的同构. 在所有的情

形下，均有 $\{uz, u\}$ 是格 $L(z')$ 的一组基．换句话说，存在

$$\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbf{Z}),$$

使得

$$\begin{pmatrix} uz \\ u \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} z' \\ 1 \end{pmatrix}.$$

对于情形 (1) 和 (2), 在 $\mathbf{C}/L(z')$ 中关系

$$uP(z) = \frac{u}{N} = \frac{cz'+d}{N} = P(z') = \frac{1}{N}$$

成立的充要条件是

$$c \equiv 0 \pmod N \quad 和 \quad d \equiv 1 \pmod N.$$

又因 $\det \gamma = ad - bc = 1$, 所以由 c 和 d 的同余条件可知

$$a \equiv 1 \pmod N.$$

这就证明了 (2). 对于 (1), 再利用第二个关系：

$$uQ(z) = \frac{uz}{N} = \frac{az'+b}{N} = Q(z') = \frac{z'}{N}$$

在 $\mathbf{C}/L(z')$ 中成立的充要条件是

$$a \equiv 1 \pmod N \quad 和 \quad b \equiv 0 \pmod N,$$

进而可知其结论正确.

类似地，在 (3) 中，关系式

$$uC(z) = \left\langle \frac{u}{N} \right\rangle = \left\langle \frac{cz'+d}{N} \right\rangle = C(z') = \left\langle \frac{1}{N} \right\rangle$$

成立当且仅当 $c \equiv 0 \pmod N$ 和 $\gcd(d, N) = 1$ 成立．而后一个关系可由 $\det\gamma = 1$ 和 $c \equiv 0 \pmod N$ 得出．这就证明了 (3).

定理 1 解释了 $\mathfrak{H}/\Gamma(N), \mathfrak{H}/\Gamma_1(N)$ 和 $\mathfrak{H}/\Gamma_0(N)$ 称为模曲线的缘由.

再回到对 Γ 的同余子群的讨论. 注意到 $\Gamma(N)$ 是 Γ 的正规子群, $\Gamma_1(N)$ 是 $\Gamma_0(N)$ 的正规子群, 并且

$$\Gamma_0(N)/\Gamma_1(N) \cong \left\{ \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} \in \mathrm{SL}_2(\mathbf{Z}/N\mathbf{Z}) \right\} \cong (\mathbf{Z}/N\mathbf{Z})^\times .$$

通过算子 "$|_k$" 将 $\Gamma_0(N)$ 作用于 $\mathcal{M}(\Gamma_1(N),k)$ 上, 得到一个 $(\mathbf{Z}/N\mathbf{Z})^\times$ 在 $\mathcal{M}(\Gamma_1(N),k)$ 上的表示, 并且它保持尖点形式不变. 于是, 对 $(\mathbf{Z}/N\mathbf{Z})^\times$ 的一个特征标 χ, 定义空间 $\mathcal{M}(\Gamma_1(N),k)$ 的子空间 $\mathcal{M}(N,k,\chi)$ 为由所有在 $\mathfrak{H}$ 上满足模形式定义中的条件 (1) 和 (3), 以及下述条件

$$(2')\ (f|_k\gamma)(z) = \chi(d)f(z), \quad \gamma = \begin{pmatrix} * & * \\ c & d \end{pmatrix} \in \Gamma_0(N)$$

的函数 f 组成. 这样的函数也称为**权 k 、水平 N 和特征标 χ 的模形式**. 从而当 χ 跑遍 $(\mathbf{Z}/N\mathbf{Z})^\times$ 的所有特征标时, 空间 $\mathcal{M}(\Gamma_1(N),k)$ 可以分解为子空间 $\mathcal{M}(N,k,\chi)$ 的直和. 同样的结论对尖点形式也成立. 需要指出的是, 当 $\chi=\chi_0$ 是 $(\mathbf{Z}/N\mathbf{Z})^\times$ 的平凡特征标时,

$$\mathcal{M}(N,k,\chi_0) = \mathcal{M}(\Gamma_0(N),k).$$

设 $h = \begin{pmatrix} N & 0 \\ 0 & 1 \end{pmatrix}$. 定义

$$\begin{aligned}\widetilde{\Gamma}(N) &= h^{-1}\Gamma(N)h \\ &= \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbf{Z}) : a \equiv d \equiv 1 \pmod N, c \equiv 0 \pmod{N^2} \right\} \\ &\subseteq \Gamma_0(N^2).\end{aligned}$$

从而空间 $\mathcal{M}(\widetilde{\Gamma}(N),k)$ 可以分解为空间 $\mathcal{M}(N^2,k,\chi)$ 的直和, 其中 χ 跑遍 $(\mathbf{Z}/N^2\mathbf{Z})^\times$ 的这样一些特征标, 它们对模 N 同余于 1 的数是平凡的. 另一方面, 映射 $f \longmapsto f|_k h$ 给出了一个从 $\mathcal{M}(\Gamma(N),k)$ 到 $\mathcal{M}(\widetilde{\Gamma}(N),k)$ 的同构. 于是对群 $\Gamma(N)$, $\Gamma_1(N)$ 和 $\Gamma_0(N)$ 上模形式的研究都归结为对空间 $\mathcal{M}(N,k,\chi)$ 的研究. 最后, 我们需要说明的是, 利用 Riemann-Roch 定理可以证明, 当 $k>2$ 时, 空间

$\mathcal{M}(N,k,\chi)$ 是 $\mathbf{C}$ 上的有限维线性空间.

§2　Hecke 算子

由于 $\Gamma_0(N)$ 包含有 $\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}$. 所以 $\mathcal{M}(N,k,\chi)$ 中任意元素 $f(z)$ 均有 Fourier 展开

$$f(z)=\sum_{n=0}^{\infty}a_n\mathrm{e}^{2\pi\mathrm{i}nz},$$

并且当 $f(z)$ 在 $\mathrm{i}\infty$ 处为 0 时有 $a_0=0$. 研究模形式 f 的 Fourier 系数 a_n 的算术性质是经典模形式理论的重要内容. 第一个问题就是算术函数 $n\longmapsto a_n$ 是否是积性函数？为此引入一个与 f 相关的 Dirichlet 级数:

$$D(s,f)=\sum_{n=1}^{\infty}a_n n^{-s}.$$

在 $\mathbf{Q}$ 的一个位 p 处, 如果存在复数 $c_1,c_p,c_{p^2},\cdots$, 使得

$$D(s,f)=\left(\sum_{p\nmid n}a_n n^{-s}\right)\left(\sum_{n=1}^{\infty}c_{p^r}p^{-rs}\right).\tag{2.1}$$

换句话说, 对任意正整数 r 和与 p 互素的正整数 n, 皆有 $a_{np^r}=a_nc_{p^r}$, 那么我们称 $D(s,f)$ 在 p 处有**Euler 积**. 于是对前述问题的研究就转化为研究 $D(s,f)$ 在何种条件下有 Euler 积. 为讨论此问题, E. Hecke 对每个不能整除水平 N 的素数 p 定义了下列算子 $\mathbb{T}_p$:

$$\mathbb{T}_p=p^{\frac{k}{2}-1}\left(\sum_{u=0}^{p-1}\begin{pmatrix}1 & u\\ 0 & p\end{pmatrix}+\chi(p)\begin{pmatrix}p & 0\\ 0 & 1\end{pmatrix}\right),$$

这就是所谓的**Hecke 算子**, 它以 $|_k\mathbb{T}_p$ 的方式作用于空间 $\mathcal{M}(N,k,\chi)$ 上.

习题 8 (1) 证明 Hecke 算子 $\mathbb{T}_p$ 映空间 $\mathcal{M}(N,k,\chi)$ 为它本身，即 $\mathbb{T}_p$ 是 $\mathcal{M}(N,k,\chi)$ 的一个线性算子. 此外证明 $\mathbb{T}_p$ 映尖点形式为尖点形式.

(2) 若模形式 $f\in\mathcal{M}(N,k,\chi)$ 有 Fourier 展开

$$f(z)=\sum_{n=0}^{\infty}a_n\mathrm{e}^{2\pi inz}.$$

证明

$$f|_k\mathbb{T}_p(z)=\sum_{n\geq 0}(a_{np}+\chi(p)p^{k-1}a_{n/p})\mathrm{e}^{2\pi inz},$$

其中当 x 不是整数时，定义 $a_x=0$.

(3) 对任意两个不能整除 N 的不同素数 p 和 p', 证明 Hecke 算子 $\mathbb{T}_p$ 和 $\mathbb{T}_{p'}$ 交换. 即

$$(f|_k\mathbb{T}_p)|_k\mathbb{T}_{p'}=(f|_k\mathbb{T}_{p'})|_k\mathbb{T}_p.$$

定理 2(Hecke) 设 $f\in\mathcal{M}(N,k,\chi)$, 且 $D(s,f)\neq 0$. 又设 p 是一个不能整除 N 的素数. 则 $D(s,f)$ 在 p 处有 Euler 积 (2.1) 的充分必要条件是，f 是 $\mathbb{T}_p$ 的特征函数. 进一步，若 $D(s,f)$ 在 p 处有 Euler 积 (2.1), 则 Euler 因子有下面表示形式:

$$\sum_{r=0}^{\infty}c_{p^r}p^{-rs}=\frac{1}{1-c_pp^{-p}+\chi(p)p^{k-1-2s}},$$

并且 $f|_k\mathbb{T}_p=c_pf$, 即 c_p 是特征值.

为证明定理，先引入下述引理.

引理 1 设 $f(z)=\sum\limits_{n=0}^{\infty}a_n\mathrm{e}^{2\pi inz}$ 是 $\mathcal{M}(N,k,\chi)$ 中的一模形式，p 是一个不整除 N 的素数. 则

(1) 若对任意与 p 互素的 n 有 $a_n=0$, 则 $f=0$. 特别地，若 $D(s,f)\neq 0$, 则存在一些与 p 互素的正整数 n, 使得 $a_n\neq 0$.

(2) 若对任意的 n 均有 $a_{np}=0$, 则 $f=0$.

证　(1) 由假设，$f(z)=\sum_{n=0}^{\infty}a_{np}e^{2\pi inpz}$. 于是

$$f(z)=f\left(z+\frac{1}{p}\right)=f|_k\begin{pmatrix}p&1\\0&p\end{pmatrix}(z).$$

另一方面，由于 N,p 互素，所以总可找到整数 a 和 c, 使得

$$ap+cN=1.$$

令

$$\gamma_1=\begin{pmatrix}1&0\\-pcN&1\end{pmatrix},\quad \gamma_2=\begin{pmatrix}a&-1\\cN&p\end{pmatrix}.$$

则

$$\gamma_1\begin{pmatrix}p&1\\0&p\end{pmatrix}\gamma_2=\begin{pmatrix}1&0\\0&p^2\end{pmatrix},$$

以及 $f|_k\gamma_1=f$, $f|_k\gamma_2=\chi(p)f$ (注意 $\gamma_1,\gamma_2\in\Gamma_0(N)$). 于是

$$\begin{aligned}\chi(p)f(z)&=f|_k\gamma_1\begin{pmatrix}p&1\\0&p\end{pmatrix}\gamma_2(z)=f|_k\begin{pmatrix}1&0\\0&p^2\end{pmatrix}(z)\\&=p^{-k}f\left(\frac{z}{p^2}\right).\end{aligned}$$

代入 f 的 Fourier 展开式得

$$\sum_{n=0}^{\infty}a_{np}e^{2\pi inz/p}=\chi(p)p^k\sum_{n=0}^{\infty}a_{np}e^{2\pi inpz}.$$

若 f 不为 0, 我们只需比较上式两边第一个不为 0 的项就得出矛盾.

(2) 假设对所有 n, 均有 $a_{np}=0$ 成立，则

$$\begin{aligned}f|_k\mathbb{T}_p(z)&=\chi(p)p^{k-1}\sum_{n\geq 0}a_{n/p}e^{2\pi inz}\\&=\chi(p)p^{k-1}\sum_{n\geq 0}b_{np}e^{2\pi inpz}\in\mathcal{M}(N,k,\chi),\end{aligned}$$

其中 $b_{np}=a_n$. 由引理的第一部分可知 $f|_k\mathbb{T}_p=0$. 即对任意的 n, $a_n=0$. 于是 $f=0$.

下面我们来证明定理 2. 记

$$f(z)=\sum_{n\geq 0}a_n\mathrm{e}^{2\pi\mathrm{i}nz}.$$

首先假定 $D(s,f)$ 在 p 处有 Euler 积. 则对任意与 p 互素的整数 m 和任意非负整数 r, 有 $a_{mp^r}=a_m c_{p^r}$. 注意到

$$\begin{aligned}(f|_k\mathbb{T}_p-c_pf)(z)&=\sum_{n\geq 0}(a_{np}+\chi(p)p^{k-1}a_{n/p}-c_pa_n)\mathrm{e}^{2\pi\mathrm{i}nz}\\&=\sum_{n\geq 0}b_n\mathrm{e}^{2\pi\mathrm{i}nz}\end{aligned}$$

仍是 $\mathcal{M}(N,k,\chi)$ 中的模形式, 并且当 p 不整除 n 时, 有

$$b_n=a_{np}+\chi(p)p^{k-1}a_{n/p}-c_pa_n=a_{np}-c_pa_n=0.$$

于是由引理 1 (1) 知函数 $f|_k\mathbb{T}_p-c_pf=0$. 所以 f 是 $\mathbb{T}_p$ 的特征函数, c_p 为其特征值. 反过来, 设 $f|_k\mathbb{T}_p-c_pf=0$, 则

$$a_{np}=c_pa_n-\chi(p)p^{k-1}a_{n/p},\qquad n\geq 0.$$

这就证明了对任意与 p 互素的整数 n, 有 $a_{np}=a_nc_p$. 从而归纳得出 $a_{np^r}=a_nc_{p^r}$, 其中 c_{p^r} 满足递推关系

$$c_{p^{r+1}}=c_pc_{p^r}-\chi(p)p^{k-1}c_{p^{k-1}}.$$

由此可以推出

$$\sum_{r=0}^{\infty}c_{p^r}p^{-rs}=\frac{1}{1-c_pp^{-s}+\chi(p)p^{k-1-2s}}.$$

从而完成了定理的证明.

在更深入的讨论研究之前, 我们先介绍一些尖点形式的性质.

命题 1 (1) 设 $f\in\mathcal{M}(N,k,\chi)$ 是一个模形式, 则 f 为尖点形式的充要条件是, 存在一个与 z 无关的常数 M, 使得

$$y^{k/2}|f(z)|<M,$$

其中 y 是 $z\in\mathfrak{H}$ 的虚部.

(2) 若 $f(z)=\sum\limits_{n=1}^{\infty}a_n\mathrm{e}^{2\pi\mathrm{i}nz}\in\mathcal{C}(N,k,\chi)$ 是尖点形式，则

$$a_n=O(n^{k/2}).$$

这两个结论的证明都很容易，我们留给读者练习.

注　推论给出的 Fourier 系数 a_n 的界远不是最好的. 由 P. Deligne 所证明的 Ramanujan-Petersson 猜想告诉我们：指数 $k/2$ 可以改进为 $(k-1)/2+\varepsilon$, 这里 $\varepsilon>0$ 为任意常数. 我们在下一节还将讨论这方面的问题.

设 H 是 Γ 的一个有限阶子群，其基本区域为 $\mathcal{D}(H)$. 设 ω 和 ω' 是紧 Rielnmann 面 $\widehat{\mathfrak{H}/H}$ 上的两个全纯 1- 形式. 则 $\omega\wedge\omega'$ 是一个 2- 形式. 在 $\mathcal{D}(H)$ 上积分这个 2- 外微分形式就得到一个确定的数，从而这就自然地定义了一个微分形式的内积 $\langle\omega,\omega^*\rangle$. 或等价地，定义了 $\mathfrak{H}$ 上权 2 的尖点形式的内积. 将此推广到 $\mathfrak{H}$ 上权 k 的模形式，我们就得到了下面所谓的 **Petersson 内积**$\langle\ ,\ \rangle$ 的定义. 对 $f,g\in\mathcal{M}(H,k)$, 定义

$$\begin{aligned}\langle f,g\rangle&=\frac{1}{[\mathrm{SL}_2(\mathbf{Z}):H]}\int_{\mathcal{D}(H)}f(x+\mathrm{i}y)\overline{g(x+\mathrm{i}y)}y^k\frac{\mathrm{d}x\mathrm{d}y}{y^2}\\&=\frac{1}{[\mathrm{SL}_2(\mathbf{Z}):H]}\frac{\mathrm{i}}{2}\int_{\mathfrak{H}/H}f(z)\overline{g(z)}(\mathrm{Im}z)^{k-2}\mathrm{d}z\wedge\mathrm{d}\bar{z}.\end{aligned}$$

这里用除以 H 在 $\mathrm{SL}_2(\mathbf{Z})$ 中的阶 $[\mathrm{SL}_2(\mathbf{Z}):H]$ 来规范化内积的目的是使得该内积的定义不依赖于 H 的选择. 当积分收敛时，上述公式的定义显然是合理的.

习题 9　证明：当 f 和 g 均为尖点形式时，内积公式中的积分是收敛的.

事实上，f 和 g 中只要有一个是尖点形式时，上述积分就是收敛的. 其实，为了研究该积分的敛散性，我们只需讨论在 $\mathcal{D}(H)$ 的每个尖点附近该积分的收敛性，而这一点通过模形式与尖点形式在尖点附近的数量阶的简单讨论就不难得出，请有兴趣的读者自已完成.

Petersson 证明了 Hecke 算子关于此内积有着很好的性质.

定理 3(Petersson) 设 p 是与 N 互素的素数. 则对于 $C(N,k,\chi)$ 中两个尖点形式 f 和 g, 有

$$\langle f|\mathbb{T}_p, g\rangle = \chi(p)\langle f, g|\mathbb{T}_p\rangle.$$

这个定理表明, 对每个素数 $p\nmid N$, Hecke 算子 $\mathbb{T}_p$ 关于 Petersson 内积是斜 Hermite 的. 于是它可以对角化. 进一步, 由于不同的 Hecke 算子是可交换的, 所以我们可以将它们联立对角化. 即我们可在 $\mathcal{M}(N,k,\chi)$ 中找到一组基, 其中每个元素都是所有 Hecke 算子的特征函数.

在证明这个定理之前,我们将用双边陪集的语言重新描述 Hecke 算子 $\mathbb{T}_p$ 的定义. 设

$$M_p(N) = \left\{ m = \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a,b,c,d \in \mathbf{Z}, \right.$$
$$\left. m \equiv \begin{pmatrix} 1 & * \\ 0 & p \end{pmatrix} (\mathrm{mod}\, N),\ \det m = p \right\}.$$

引理 2 设 $R_p = \begin{pmatrix} a & -1 \\ cN & p \end{pmatrix} \in \Gamma_0(N)$, 这里 a, c 是使 $ap + cN = 1$ 成立的两个给定的整数. 则

$$M_p(N) = \Gamma_1(N) \begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix} \Gamma_1(N)$$
$$= \bigcup_{u=0}^{p-1} \Gamma_1(N) \begin{pmatrix} 1 & u \\ 0 & p \end{pmatrix} \bigcup \Gamma_1(N)\, R_p \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix}.$$

证 由于

$$R_p \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix} \begin{pmatrix} pa & -1 \\ cN & 1 \end{pmatrix} \in \begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix} \Gamma_1(N),$$

所以显然有

$$M_p(N) \supseteq \Gamma_1(N) \begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix} \Gamma_1(N)$$

$$\supseteq \bigcup_{u=0}^{p-1} \Gamma_1(N)\begin{pmatrix}1 & u\\ 0 & p\end{pmatrix} \bigcup \Gamma_1(N)R_p\begin{pmatrix}p & 0\\ 0 & 1\end{pmatrix}.$$

下面任取 $m=\begin{pmatrix}a' & b'\\ c' & d'\end{pmatrix}\in M_p(N)$. 若 a' 和 c' 互素，取 $x,y\in\mathbf{Z}$, 使得 $xa'+yc'=1$. 则 $\begin{pmatrix}x & y\\ -c' & a'\end{pmatrix}\in\Gamma_1(N)$, 且

$$\begin{pmatrix}x & y\\ -c' & a'\end{pmatrix}\begin{pmatrix}a' & b'\\ c' & \alpha'\end{pmatrix}=\begin{pmatrix}1 & *\\ 0 & p\end{pmatrix}.$$

这表明 $m\in\Gamma_1(N)\begin{pmatrix}1 & u\\ 0 & p\end{pmatrix}$, 其中 $u\equiv *\pmod p$. 若 a' 和 c' 不互素，由于 $\det m=p$, $\gcd(a',c')|\det m$. 故

$$\gcd(a',c')=p.$$

由此容易验证，$m\in\Gamma_1(N)R_p\begin{pmatrix}p & 0\\ 0 & 1\end{pmatrix}$. 引理得证.

注意到算子 R_p 在 $\mathcal{C}(N,k,\chi)$ 的作用相当于乘上一个 $\chi(p)$. 于是 Hecke 算子 $\mathbb{T}_p$ 可以表成

$$\mathbb{T}_p=p^{\frac{k}{2}-1}\sum_i\alpha_i,$$

其中 $\{\alpha_i : i=1,2,\cdots\}$ 是 $\Gamma_1(N)$ 在 $M_p(N)$ 中的任意一组右陪集代表，即

$$M_p(N)=\bigcup_i\Gamma_1(N)\alpha_i.$$

对矩阵 $m=\begin{pmatrix}a & b\\ c & d\end{pmatrix}$, 我们以 m' 表示矩阵 $\begin{pmatrix}d & -b\\ -c & a\end{pmatrix}$. 即当 m 可逆时，$m'=(\det m)m^{-1}$. 由

$$\begin{aligned}R_p\begin{pmatrix}1 & 0\\ 0 & p\end{pmatrix}' &= R_p\begin{pmatrix}p & 0\\ 0 & 1\end{pmatrix}\\ &=\begin{pmatrix}1 & 0\\ 0 & p\end{pmatrix}\begin{pmatrix}ap & -1\\ cN & 1\end{pmatrix}\in\begin{pmatrix}1 & 0\\ 0 & p\end{pmatrix}\Gamma_1(N)\end{aligned}$$

可知 $M_p(N)=R_pM_p(N)'$.

由于 $M_p(N)$ 是 $\Gamma_1(N)$ 的一个双陪集，故 $M_p(N)$ 中任意一个 $\Gamma_1(N)$ 的左陪集同任意一个 $\Gamma_1(N)$ 的右陪集相交不空. 于是存在 $\alpha_1,\cdots,\alpha_{p+1}\in M_p(N)$, 它们既是左陪集表示也是右陪集表示的代表元，即

$$M_p(N)=\bigcup_i \Gamma_1(N)\alpha_i=\bigcup_i \alpha_i\Gamma_1(N).$$

从而

$$\begin{aligned}M_p(N)&=\bigcup_i \Gamma_1(N)\alpha_i=\bigcup_i R_p(\alpha_i\Gamma_1(N))'\\&=\bigcup_i \Gamma_1(N)\ R_p\alpha_i'.\end{aligned}$$

所以我们有

$$\mathbb{T}_p=p^{\frac{k}{2}-1}\sum_i \alpha_i=p^{\frac{k}{2}-1}\sum_i R_p\alpha_i'.$$

这样我们就知道等式

$$\langle f|_k\mathbb{T}_p,g\rangle=\chi(p)\langle f,g|_k\mathbb{T}_p\rangle$$

等价于

$$\left\langle f|_k\sum_i\alpha_i,g\right\rangle=\left\langle f,g|_k\sum_i\alpha_i'\right\rangle.$$

于是我们把问题归结为对任意的 $\alpha\in M_p(N)$, 证明

$$\langle f|_k\alpha,g\rangle=\langle f,g|_k\alpha'\rangle.$$

习题 10 设 $\alpha\in M_p(N)$, 证明

$$H=\alpha^{-1}\Gamma(Np)\alpha \quad 和 \quad H'=(\alpha')^{-1}\Gamma(Np)\alpha'$$

均为 $\Gamma_1(N)$ 的子群，且它们关于群 $\Gamma=\mathrm{SL}_2(\mathbf{Z})$ 的阶均与 $\Gamma(Np)$ 关于 Γ 的阶相同. 此外，区域 $\alpha^{-1}\mathcal{D}(\Gamma(Np))$ 是 H 的一个基本区域.

习题 11 以 $\delta(f,g)(z)$ 表示微分形式

$$f(z)\overline{g(z)}(\mathrm{Im}z)^{k-2}\mathrm{d}z\wedge\mathrm{d}\overline{z}.$$

证明：对任意有正行列式值的二阶实矩阵 γ，均有

$$\delta(f|_k\gamma,g|_k\gamma)(z)=\delta(f,g)(\gamma z).$$

给出 $M_p(N)$ 中一个元 α, 由习题 10 知，$f|_k\alpha$, $g|_k\alpha'$, f 和 g 均为 $\Gamma(Np)$ 上的尖点形式. 此外 $f|_k\alpha$ 和 g 也是群 $H=\alpha^{-1}\Gamma(Np)\alpha$ 上的尖点形式，设

$$n=[\mathrm{SL}_2(\mathbf{Z}):H]=[\mathrm{SL}_2(\mathbf{Z}):\Gamma(Np)],$$

由定义可得

$$\begin{aligned}\langle f|_k\alpha,g\rangle&=\frac{\mathrm{i}}{2n}\iint\limits_{\mathcal{D}(H)}\delta(f|_k\alpha,g)(z)\\&=\frac{\mathrm{i}}{2n}\iint\limits_{\alpha^{-1}\mathcal{D}(\Gamma(N_p))}\delta(f|_k\alpha,g)(z)\\&=\frac{\mathrm{i}}{2n}\iint\limits_{\mathcal{D}(\Gamma(N_p))}\delta(f|_k\alpha,g)(\alpha^{-1}z)\\&=\frac{\mathrm{i}}{2n}\iint\limits_{\mathcal{D}(\Gamma(N_p))}\delta(f|_k\alpha|_k\alpha^{-1},g|_k\alpha^{-1})(z)\\&=\frac{\mathrm{i}}{2n}\iint\limits_{\mathcal{D}(\Gamma(N_p))}\delta(f,g|_k\alpha')(z)\\&=\langle f,g|_k\alpha'\rangle.\end{aligned}$$

由此定理 3 得证.

推论 1 设 p 是一个不能整除 N 的素数. 当 $\chi(p)=1$ 时, Hecke 算子 $\mathbb{T}_p$ 在空间 $C(N,k,\chi)$ 中的所有特征值均是实的; 当 $\chi(p)=-1$ 时，这些特征值均是纯虚数. 一般地说，$\mathbb{T}_p$ 在 $C(N,k,\chi)$ 中的特征值 λ_p 满足关系 $\overline{\lambda}_p=\overline{\chi(p)}\lambda_p$.

注 用双陪集定义 Hecke 算子想法的抽象化就产生了 Hecke 环理论. 这方面系统论述可以参阅 G. Shimura[29] 和 A.N. Andrianov[1].

§3 空间 $\mathcal{M}(N,k,\chi)$ 的结构

我们首先研究尖点形式空间 $\mathcal{C}(N,k,\chi)$ 的结构. 设 M 是一个可整除 N 的整数, χ 为模 M 的特征标, 显然, 空间 $\mathcal{C}(M,k,\chi)$ 包含在 $\mathcal{C}(N,k,\chi)$ 中. 设 d 是一个正整数, 定义算子

$$B_d = d^{-k/2}\begin{pmatrix} d & 0 \\ 0 & 1 \end{pmatrix},$$

它对 H 上的全纯函数 f 的作用是

$$(f|_k\, B_d)(z) = d^{-k/2} f|_k \begin{pmatrix} d & 0 \\ 0 & 1 \end{pmatrix}(z) = f(dz).$$

习题 12 (1) 证明: B_d 把空间 $\mathcal{M}(N,k,\chi)$ 映入 $\mathcal{M}(Nd,k,\chi)$, 且映尖点形式为尖点形式.

(2) 对一个不能整除 Nd 的素数 p, 有 $B_d\mathbb{T}_p = \mathbb{T}_p B_d$, 且它们均把空间 $\mathcal{M}(Nd,k,\chi)$ 映入 $\mathcal{M}(Nd,k,\chi)$.

于是对 N/M 的任意正因子 d, $\mathcal{C}(M,k,\chi)|_k B_d$ 包含在 $\mathcal{C}(N,k,\chi)$ 中, 由于通过一个简单的变量代换 $z \longmapsto dz$, 我们可将级 M 的模形式提升成级 dM 的形式, 所以我们称空间 $\mathcal{C}(M,k,\chi)|_k B_d$ 中的尖点形式是空间 $\mathcal{C}(M,k,\chi)$ 中尖点形式的"提升". 用 $\mathcal{C}^-(N,k,\chi)$ 表示由 $\mathcal{C}(M,k,\chi)$ 中的模形式以及它们通过 B_d 提升后的模形式张成的空间, 其中 M 跑遍所有使得 χ 为模 M 的特征标的 N 的正因子, d 是 N/M 的任意正因子. 空间中的元素称为**旧形式**. 由习题 12(2) 知, Hecke 算子 $\mathbb{T}_p$ 映旧形式为旧形式. 又由定理 3 可知, 空间 $\mathcal{C}^-(N,k,\chi)$ 可以分解为所有 Hecke 算子 $\mathbb{T}_p, p\nmid N$ 的公共特征空间的直和. 设 $f \in \mathcal{C}(M,k,\chi)$ 是所有 Hecke 算子 $\mathbb{T}_p(p\nmid N)$ 的公共特征函数. 由习题 12(2) 可以看出, 对于任意的 $d\,|\,(N/M)$, $f|_k B_d$ 也是所有 Hecke 算子的公共特征函数, 并且它与 f 有同样的特征

值. 因此, $C^-(N,k,\chi)$ 中每个公共特征空间的维数均大于 1.

容易验证, $C(N,k,\chi)$ 关于 Petersson 内积是一个 Hilbert 空间, 我们以 $C^+(N,k,\chi)$ 表示 $C^-(N,k,\chi)$ 在空间 $C(N,k,\chi)$ 中的正交补, 由定理 3 知, 它仍然是所有 Hecke 算子 $\mathbb{T}_p\,(p\nmid N)$ 的不变子空间, 从而它也可以分解为具有 Hecke 的公共特征空间的直和. 在每个这样的公共特征空间中, 任何一个非零形式的水平正好是 N, 故称它们为**权 k 、水平为 N 、特征标为 χ 的新形式**. 这样空间 $C(N,k,\chi)$ 可以由权 k 、水平为 M 及特征标为 χ 的新形式, 以及它们通过 B_d 提升后的元素生成, 其中 $M|N$ 且 χ 为模 M 的特征标, d 过所有 N/M 的正因子. 新形式的第一个特点是它所处的公共特征空间一定是一维的. 严格地讲, 就是下面定理.

定理 4 (1) 设 $f(z)=\sum\limits_{n=1}^{\infty}a_n\mathrm{e}^{2\pi\mathrm{i}nz}$ 是一个权 k 、水平 N 及特征标为 χ 的新形式. 则 $a_1\neq 0$. 于是我们可假定 f 是正规化的, 即 $a_1=1$. 则对任意素数 $p\nmid N$, $f|_k\mathbb{T}_p=a_pf$, 即 a_p 是 $\mathbb{T}_p$ 关于 f 的特征值.

(2) 设 $f(z)=\sum\limits_{n=1}^{\infty}a_n\mathrm{e}^{2\pi\mathrm{i}nz}$, $g(z)=\sum\limits_{n=1}^{\infty}b_n\mathrm{e}^{2\pi\mathrm{i}nz}$ 是两个正规化的权为 k, 特征标为 χ 且水平分别为 N 和 M 的新形式. 其中 $M|N$, 则存在无穷多个素数 $p\nmid N$, 使得 $a_p\neq b_p$.

证 (1) 对素数 $p\nmid N$, 设 λ_p 是 Hecke 算子 $\mathbb{T}_p$ 关于 f 的特征值, 即 $f|_k\mathbb{T}_p=\lambda_pf$. 由定理 2 知, $a_p=a_1\lambda_p$. 于是当 $a_1=1$ 时, $a_p=\lambda_p$. 从而剩下的问题均归结为证明 $a_1\neq 0$. 如若不然, 再次利用定理 2 知 $a_{p^r}=a_1c_{p^r}=0$ 对任意的 $p\nmid N$ 和 $r\geq 0$ 均成立, 进而对任意与 N 互素, 且互不相同的素数 $p_1,\cdots,p_l$, 和非负整数 $r_1,\cdots,r_l$, 有

$$a_{p_1^{r_1}\cdots p_1^{r_l}}=a_{p_1^{r_1}}\cdots a_{p_l^{r_l}}=0.$$

换句话说, 对任意与 N 互素的整数 n, 均有 $a_n=0$.

(2) 假设 f 和 g 分别为水平为 N 和 M 的正规化的模形式,

并且对几乎所有的 $p\nmid N$, f 和 g 关于 Hecke 算子 $\mathbb{T}_p$ 有相同的特征值. 则

$$h(z)=f(z)-g(z)=\sum_{n=1}^{\infty}c_n e^{2\pi i n z}\in \mathcal{C}(N,k,\chi),$$

且对几乎所有的 Hecke 算子 $\mathbb{T}_p$, $h(z)$ 是 $\mathbb{T}_p$ 的特征函数, 并且 $c_1=0$. 用与 (1) 同样的方法可以证明, 存在一个正整数 K, 使得当 n 与 K 互素时有 $c_n=0$.

综上所述, 定理 4 的证明依赖下述结果:

定理 4′ 设

$$f(z)=\sum_{n=1}^{\infty}a_n e^{2\pi i n z}\in \mathcal{C}(N,k,\chi).$$

若存在一个无平方因子的正整数 K, 使得对所有与 K 互素的整数 n, 都有 $a_n=0$, 则 $f\in \mathcal{C}^-(N,k,\chi)$.

假设定理 4′ 成立, 我们继续讨论定理 4 的证明. 对 (1), 若 $a_1=0$, 则

$$f\in \mathcal{C}^+(N,k,\chi)\bigcap \mathcal{C}^-(N,k,\chi)=\{0\}.$$

故 $f=0$, 与假设矛盾. 对 (2), 若 $M=N$, 则

$$f-g\in \mathcal{C}^+(N,k,\chi)\bigcap \mathcal{C}^-(N,k,\chi),$$

于是 $f=g$; 若 $M\neq N$, 则 $f-g$ 和 g 均为 $\mathcal{C}^-(N,k,\chi)$ 中元. 从而 $f\in \mathcal{C}^-(N,k,\chi)$. 于是 $f=0$. 与假设矛盾, 由此就完成了定理 4 的证明.

习题 13 证明每个新形式的公共特征空间的维数均为 1.

为证明定理 4′, 我们需要做些准备. 首先我们讨论与引理 1 的互补的问题.

引理 3 设模形式 $f(z)=\sum_{n=1}^{\infty}a_{nq}e^{2\pi i nqz}\in \mathcal{C}(N,k,\chi)$, 其中 q 是一个可整除 N 的素数.

(1) 若 χ 是一个模 N/q 的特征标，则

$$g(z) = \sum_{n=1}^{\infty} a_{nq} e^{2\pi i n z} \in C(N/q, k, \chi).$$

(2) 若 χ 不是一个模 N/q 的特征标，则 $f = 0$.

证 注意到

$$g(z) = \sum_{n=1}^{\infty} a_{nq} e^{2\pi i n z} = q^{\frac{k}{2}} f|_k \begin{pmatrix} 1 & 0 \\ 0 & q \end{pmatrix} (z).$$

对 $\Gamma_0(N)$ 中元 $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$, 有

$$\begin{pmatrix} 1 & 0 \\ 0 & q \end{pmatrix}^{-1} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & q \end{pmatrix} = \begin{pmatrix} a & bq \\ c/q & d \end{pmatrix}.$$

以 $\Gamma_0(N/q, q)$ 表示集

$$\begin{pmatrix} 1 & 0 \\ 0 & q \end{pmatrix}^{-1} \Gamma_0(N) \begin{pmatrix} 1 & 0 \\ 0 & q \end{pmatrix},$$

则对 $\Gamma_0(N/q, q)$ 中任意元素 $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$, 显然有

$$g|_k \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \chi(d) g.$$

特别地，函数 g 在群

$$\Gamma(N/q, q) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N/q, q) : \ a \equiv d \equiv 1 \ (\mathrm{mod}\ N) \right\}$$

中的元素以及 $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ 的作用下不变.

(1) 若 χ 是模 N/q 的特征标，则 g 在 $\Gamma_1(N/q)$ 作用下不变. 又设 $\Gamma_0(N/q)$ 关于子群 $\Gamma_0(N/q, q)$ 有陪集表示

$$\Gamma_0(N/q) = \bigcup_i R_i \Gamma_0(N/q, q).$$

容易验证，这些 R_i 可从 $\Gamma_1(N/q)$ 中取．于是任取

$$\gamma=\begin{pmatrix}x & y\\ z & w\end{pmatrix}\in\Gamma_0(N/q),$$

记 $\gamma=\gamma' R_i$，其中

$$\gamma'=\begin{pmatrix}x' & y'\\ z' & w'\end{pmatrix}\in\Gamma_0(N/q,q).$$

我们发现 $w\equiv w' \pmod{N/q}$，这样

$$g|_k\,\gamma=g|_k\,\gamma'|_k\,R_i=\chi(w')g=\chi(w)g.$$

由此表明， $g\in\mathcal{C}(N/q,\ k,\ \chi)$．

(2) 若 χ 不是模 N/q 的特征标，由于

$$\begin{pmatrix}1 & q\\ N/q & N+1\end{pmatrix}\in\Gamma_0(N/q,q).$$

故对任意的整数 u 和 u'，g 在

$$\begin{pmatrix}1 & u\\ 0 & 1\end{pmatrix}\begin{pmatrix}1 & q\\ N/q & N+1\end{pmatrix}\begin{pmatrix}1 & u'\\ 0 & 1\end{pmatrix}$$

$$=\begin{pmatrix}1+uN/q & u'(1+uN/q)+q+uN+u\\ N/q & u'N/q+N+1\end{pmatrix}$$

$$=\begin{pmatrix}A & B\\ C & D\end{pmatrix}$$

作用下不变．由于 χ 不是模 N/q 的特征标，故存在 $u'\in\mathbf{Z}$，使得

$$u'N/q+1\not\equiv 0 \pmod q,$$

且 $\chi(u'N/q+1)\neq 1$．从而，由

$$B\equiv u'(1+uN/q)+u\equiv u(1+u'N/q)+u' \pmod q$$

知，存在 $u\in\mathbf{Z}$，使得 $B\equiv 0 \pmod q$．当 u,u' 如上选定之后，有

$$\begin{pmatrix}A & B\\ C & D\end{pmatrix}\in\Gamma_0(N/q,q)$$

和

$$g = g|_k \begin{pmatrix} A & B \\ C & D \end{pmatrix} = \chi(D)g = \chi(u'N/q + 1)g.$$

这只有在 $g = 0$ 时才有可能，于是 $f = g|_k B_q = 0$. 由此引理 3 证明完毕.

接下来我们将引入两个算子. 为方便起见，今后如无特殊说明，我们总以 p 表示一个与 N 互素的素数，以 q 表示 N 的一个素因子. 在位 q 处，下面这个算子扮演了与 $\mathbb{T}_p$ 类似的角色:

$$U_q = q^{\frac{k}{2}-1} \sum_{u(\bmod q)} \begin{pmatrix} 1 & u \\ 0 & q \end{pmatrix},$$

它将 $f(z) = \sum\limits_{n=0}^{\infty} a_n e^{2\pi i n z}$ 映为

$$f|_k U_q(z) = \sum_{n=0}^{\infty} a_{nq} e^{2\pi i n z}.$$

其性质可以概括为下列习题.

习题 14 证明下面结论:

(1) U_q 将空间 $\mathcal{C}(N,k,\chi)$ 映入其本身; 并且，如果 $q^2|N$ 且 χ 是模 N/q 的特征标，那么算子 U_q 将空间 $\mathcal{C}(N,k,\chi)$ 映入空间 $\mathcal{C}(N/q,k,\chi)$.

(2) $\mathbb{T}_p U_q = U_q \mathbb{T}_p$. 此外，当 q 与 d 互素时，$U_q B_d = B_d U_q$.

由于 q 为 N 的一个素因子，所以存在 q 的一个方幂 Q, 使得

$$N = N'Q,$$

其中 N' 是一个与 Q 互素的整数. 取整数 x, y, z, 使得

$$Q^2x - Nyz = Q.$$

我们用

$$W_q^N = \begin{pmatrix} Qx & y \\ Nz & Q \end{pmatrix}$$

来定义 **Atkin-Lehner 算子** W_q^N. 把 χ 写成 $\chi_{N'} \cdot \chi_Q$ 的形式，其中 χ_M 表示模 M 的特征标. 于是算子 W_q^N 映 $\mathcal{C}(N,k,\chi_Q\chi_{N'})$ 为

$\mathcal{C}(N,k,\overline{\chi}_Q\chi_{N'})$. 不过这个算子依赖于 x,y,z 的选取. 然而, 如果 χ_Q 是平凡的, 即 χ 是一个模 N/Q 的特征标, 那么我们就得到一个 $\mathcal{C}(N,k,\chi)$ 上定义合理的算子.

习题 15 证明下列结论:

(1) 假设 χ 是一个模 N/Q 特征标, 则算子

$$W_q^N:\mathcal{C}(N,k,\chi)\longrightarrow\mathcal{C}(N,k,\chi)$$

不依赖于 x,y,z 的选取. 此外, $W_q^N\mathbb{T}_p=\mathbb{T}_pW_q^N$, 并且对任意的 $f\in\mathcal{C}(N,k,\chi)$, 有

$$f|_kW_q^N|_kW_q^N=\chi(Q)f.$$

特别地 W_q^N 是空间 $\mathcal{C}(N,k,\chi)$ 的一个自同构.

(2) 若 $q|N$, $q^2\nmid N$, χ 是模 N/q 的特征标. 则

$$U_q+q^{k/2-1}W_q^N:\mathcal{C}(N,k,\chi)\longrightarrow\mathcal{C}(N/q,k,\chi).$$

引入这两个算子的目的是使我们能构造一些旧形式, 使得我们把它们从一个给定的模形式中减去时, 有更多的 Fourier 系数为 0.

引理 4 设 $f(z)=\sum\limits_{n=1}^{\infty}a_n\mathrm{e}^{2\pi\mathrm{i}nz}\in\mathcal{C}(N,k,\chi)$, K 是一个给定的正整数, 并且当 $\gcd(n,K)=1$ 时, $a_n=0$. 那么

(1) 当 $\gcd(n,N)=1$ 时, $a_n=0$;

(2) 若 $q|N$, 且 χ 为模 N/q 的特征标, 命

$$\psi=\begin{cases}f|_kU_q, & q^2|N \text{ 或 } (K,N)=q,\\ (1+q^{-1})^{-1}f|_k(U_q+q^{k/2-1}W_q^N), & \text{其他情况}.\end{cases}$$

则 $\psi\in\mathcal{C}(N/q,k,\chi)$ 和

$$(f-\psi|_kB_q)(z)=\sum_{n=1}^{\infty}b_n\mathrm{e}^{2\pi\mathrm{i}nz}\in\mathcal{C}(N,k,\chi),$$

并且当 $\gcd(n,K,N)=1$ 或 q 时, $b_n=0$.

证 对一个素数 l, 下面式子定义了一个零化算子 A_l：

$$f|_k A_l = f - f|_k U_l|_k B_l,$$

它将 f 的所有指数为 l 之倍数的 Fourier 系数全部化为零. 显然 $f|_k A_l \in \mathcal{C}(Nl^2, k, \chi)$, 不过当 $l|N$ 以及 χ 为模 N/l 的特征标时，级还可低一些. 事实上，在这种情况下，利用习题 14 和 12 可知，按照 $l|N$ 或 $l^2|N$, $f|_k A_l$ 位于 $\mathcal{C}(Nl, k, \chi)$ 中或 $\mathcal{C}(N, k, \chi)$ 中.

设 $l_1, \cdots, l_r$ 是 K 的所有互异的素因子，并不妨设 $l_r \nmid N$ (否则 (1) 成立). 于是由假设可知，存在一个适当的函数 $\Phi(z)$, 使得

$$f|_k A_{l_1}|_k A_{l_2}|_k \cdots |_k A_{l_{r-1}} = \Phi|_k B_{l_r} \in \mathcal{C}(Nl_1^2 \cdots l_{r-1}^2, k, \chi).$$

由引理 1 (1) 可知 $\Phi = 0$. 从而对任意 n, 只要

$$(n, l_1 \cdots l_{r-1}) = 1,$$

均有 $a_n = 0$. 由此利用归纳法我们可以证得 (1).

对于 (2), 在 $\psi = f|_k U_q$ 的情形，由于

$$\psi|_k B_q(z) = \sum_{n=1}^{\infty} a_{nq} e^{2\pi i nqz},$$

于是 $f - \psi|_k B_q$ 具有所要求的性质； 并且 $q^2|N$ 时，由习题 14(1) 可知， $\psi \in \mathcal{C}(N/q, k, \chi)$; 在 $(K, N) = q$ 时，则由引理 3(1) 可知, $\psi \in \mathcal{C}(N/q, k, \chi)$. 对于剩余的情形，我们有 $q^2 \nmid N$, 即 $\mathrm{ord}_q N = 1$, 且 $\gcd(N, K)$ 至少有两个素因子. 设 $q_1, \cdots, q_t = q$ 是 $\gcd(N, K)$ 的素因子，其中 $t \geq 2$. 由习题 15(2) 可知,

$$(1 + q^{-1})\psi = f|_k (U_q + q^{\frac{k}{2}-1} W_q^N) \in \mathcal{C}(N/q, k, \chi).$$

为证明 $f - \psi|_k B_q$ 有所要求的性质，我们只需证明：存在具有

$$\sum_{n=1}^{\infty} c_n e^{2\pi i nz}$$

形式 Fourier 展开的 $f_i(z)$, 使得

$$f - \psi|_k B_q = \sum_{i=1}^{t-1} f_i | B_{q_i}.$$

为此，我们将 f 写成

$$\sum_{i=1}^{t} \Phi_i|_k B_{q_i},$$

其中 $\Phi_1 = f|_k U_{q_1}$，当 $t \geq i \geq 2$ 时，

$$\Phi_i = f|_k A_{q_1}|_k \cdots |_k A_{q_{i-1}}|_k U_{q_i}.$$

由前面讨论知，当 $t > i \geq 1$ 时， $\Phi_i|_k B_{q_i} \in \mathcal{C}(Nq_1^2 \cdots q_i^2, k, \chi)$ 且

$$\Phi_t|_k B_q = f|_k A_{q_1}|_k \cdots |_k A_{q_{t-1}} \in \mathcal{C}(Nq_1^2 \cdots q_{t-1}^2, k, \chi).$$

再结合引理 3 (1) 就得到 $\Phi_t \in \mathcal{C}(Nq_1^2 \cdots q_{t-1}^2/q, k, \chi)$，命

$$M = Nq_1^2 \cdots q_{t-1}^2,$$

则

$$\mathrm{ord}_q M = \mathrm{ord}_q N = 1.$$

于是我们可以用 W_q^M 来代替 W_q^N. 注意到，当 $1 \leq i \leq t-1$ 时，q_i 与 q 互素. 从而有

$$B_{q_i} U_q = U_q B_{q_i} \quad 和 \quad B_{q_i} W_q^M = W_q^{M/q_i} B_{q_i},$$

于是

$$\begin{aligned}
&\Phi_i|_k B_{q_i}|_k (U_q + q^{k/2-1} W_q^M) \\
&\quad = \Phi_i|_k (U_q + q^{k/2-1} W_q^{M/q_i})|_k B_{q_i} = \Psi_i|_k B_{q_i},
\end{aligned}$$

其中 $\Psi_i = \Phi_i|_k (U_q + q^{k/2-1} W_q^{M/q_i}) \in \mathcal{C}(M/q, k, \chi)$. 由

$$B_q U_q = q^{-1} \sum_{u=0}^{q-1} \begin{pmatrix} 1 & u \\ 0 & 1 \end{pmatrix}$$

和

$$W_q^M = \begin{pmatrix} qx & y \\ Mz & q \end{pmatrix}$$

以及 $\Phi_t \in \mathcal{C}(M/q,k,\chi)$ 可得

$$\Phi_t|_k B_q|_k(U_q + q^{k/2-1}W_q^M) = \Phi_t + q^{-1}\Phi_t|_k \begin{pmatrix} qx & y \\ Mz/q & 1 \end{pmatrix}$$

$$= (1+q^{-1})\Phi_t.$$

于是

$$\begin{aligned} f - \psi|_k B_q &= \sum_{i=1}^{t} \Phi_i|_k B_{q_i} - (1+q^{-1})^{-1} \\ &\quad \times \left(\sum_{i=1}^{t-1} \Psi_i|_k B_{q_i} + (1+q^{-1})\Phi_t \right) |_k B_q \\ &= \sum_{i=1}^{t-1} \left(\Phi_i - (1+q^{-1})^{-1}\Psi_i|_k B_q \right) |_k B_{q_i} \\ &= \sum_{i=1}^{t-1} f_i|_k B_{q_i}, \end{aligned}$$

其中 $f_i \in \mathcal{C}(M,k,\chi)$. 由此即得到所述结论, 引理得证.

下面来证明定理 4′. 设 $f(z)$ 如假设所述、反复应用引理 4, 我们总可假定 $\gcd(N,K)$ 的素因子为 $q_1\cdots,q_r$, 并且 χ 不是模 N/q_i 的特征标, 以及当 $\gcd(n,q_1\cdots q_r)=1$ 时, $a_n=0$. 设

$$\Phi_r = f|_k A_{q_1}|_k \cdots |_k A_{q_{r-1}}|_k U_{q_r},$$

则

$$\Phi_r|_k B_{q_r} = f|_k A_{q_1}|_k \cdots |_k A_{q_{r-1}} \in \mathcal{C}(Nq_1^2\cdots q_{r-1}^2,k,\chi).$$

由于 χ 不是模 $Nq_1^2\cdots q_{r-1}^2/q$ 的特征标, 于是由引理 3(2) 知 $\Phi_r=0$, 这表明当 $n,q_1,\cdots,q_{r-1}$ 互素时, $a_n=0$. 利用归纳法即得 $f=0$. 这就完成了定理 4′ 的证明, 从而定理 4 也真.

习题 16 以 $\mathcal{N}(M,k,\chi)$ 表示权为 k 、水平为 M 及特征标为 χ 的新形式集合 (当这样的新形式不存在时, 取该集合为空集), 证明

$$\bigcup_{M|N}\bigcup_{d|\frac{N}{M}}\mathcal{N}(M,k,\chi)|_k B_d$$

在 $\mathbf{C}$ 上生成了空间 $\mathcal{C}(N,k;\chi)$, 并为其一组基.

设

$$f(z)=\sum_{n=1}^{\infty}a_n e^{2\pi i n z}$$

是一个正规化的权 k 、水平 N 以及特征标为 χ 的新形式, 由定理 4(1) 知, 对素数 $p\nmid N$,

$$f|_k\mathbb{T}_p=a_pf.$$

于是对任意的 $n\geq 1$ 及 $p\nmid N$ 有

$$a_{np}+\chi(p)p^{k-1}a_{n/p}=a_pa_n.$$

下面设 q 为 N 的一个素因子, 则

$$f|_kU_q(z)=\sum_{n=1}^{\infty}a_{nq}e^{2\pi i n z}\in\mathcal{C}(N,k,\chi),$$

并且对素数 $p\nmid N$, 它与 f 关于 Hecke 算子 $\mathbb{T}_p$ 有同样的特征值. 这表明函数 $f|_kU_q-a_qf$ 也有同样的性质. 由于包含 f 的公共特征空间的维数是 1, 而 $f|_kU_q-a_qf$ 的首项 Fourier 系数为 0, 于是从定理 4 (1) 可知

$$f|_kU_q=a_qf.$$

从而对任意的 $n\geq 1$ 和 $q|N$, 有

$$a_{nq}=a_qa_n.$$

下面我们更仔细地讨论一下 Fourier 系数 a_q.

情形 1: χ 是一个模 N/q 的特征标.

(1) 若 $q^2|N$, 则 $f|_kU_q=a_qf\in\mathcal{C}(N/q,k,\chi)$, 又注意到 f 是水平 N 的新形式, 所以由上面关系导出 $a_qf=0$, 即 $a_q=0$.

(2) 若 $q^2\nmid N$, 则由习题 15(2) 知

$$f|_k\left(U_q+q^{\frac{k}{2}-1}W_q^N\right)\in\mathcal{C}(N/q,k,\chi).$$

另一方面，$f|_k W_q^N$ 与 $f|_k U_q$ 一样，都是所有 Hecke 算子 $\mathbb{T}_p\,(p\nmid N)$ 的公共特征函数，且有与 f 相同的特征值. 于是

$$f|_k U_q = a_q f = -q^{\frac{k}{2}-1} f|_k W_q^N.$$

又注意到 $f|_k W_q^N|_k W_q^N = \chi(q)f$, 所以 $a_q^2 = \chi(q)q^{k-2}$.

情形 2： χ 不是一个模 N/q 的特征标. 此时，利用 A.Ogg[19] 的一个结果，可以判定 $|a_q| = q^{\frac{k-1}{2}}$. Ogg 的结果，我们将在下面论述.

引入算子

$$H_N = \begin{pmatrix} 0 & -1 \\ N & 0 \end{pmatrix}.$$

习题 17　证明：H_N 将空间 $\mathcal{C}(N,k,\chi)$ 映为 $\mathcal{C}(N,k,\overline{\chi})$, 且 $H_N^2 = \chi(-1)$. 进一步, 证明 $H_N\mathbb{T}_p = \overline{\chi}(p)\mathbb{T}_p H_N$, $p\nmid N$. 于是 H_N 映 $\mathcal{C}^-(N,k,\chi)$ 为 $\mathcal{C}^-(N,k,\overline{\chi})$, 映 $\mathcal{C}^+(N,k,\chi)$ 为 $\mathcal{C}^+(N,k,\overline{\chi})$.

再定义算子 K 为

$$f|K(z) = \overline{f(-\overline{z})}.$$

换言之，若 $f(z) = \sum\limits_{n=0}^{\infty} a_n e^{2\pi i n z}$, 则

$$f|K(z) = \sum_{n=0}^{\infty} \overline{a}_n e^{2\pi i n z}.$$

以后在不至于产生混淆时，我们也记 $f|K$ 为 $\overline{f}$. 显然，算子 K 映 $\mathcal{C}(N,k,\chi)$, 为 $\mathcal{C}(N,k,\overline{\chi})$, 且 $K^2 = \mathrm{id}$. 此外,

$$K\mathbb{T}_p = \mathbb{T}_p K,\ H_N K = (-1)^k K H_N.$$

设 g 是一个权 k, 水平 N, 特征标为 χ 的正规化的新形式, 则 $g|K = \overline{g}$ 是一个权 k, 水平 N, 但特征标为 $\overline{\chi}$ 的正规化的新形式，并且，存在常数 λ_g, 使得 $g|H_N = \lambda_g \overline{g}$.

习题 18　证明上面所述算子 K 的性质以及它同算子 $\mathbb{T}_p$ 和 H_N 的关系.

引理 5 (Ogg) 设 $q|N$, 令 $N=q^eM$, 其中 $q\nmid M$; 又设 χ 不是模 M 的特征标. 则在空间 $C(N,k,\chi)$ 中有

$$U_q^eH_NU_q^e=q^{k-1}U_q^{e-1}H_NU_q^{e-1}.$$

证 注意到

$$U_q^e=q^{e(\frac{k}{2}-1)}\sum_{u(\operatorname{mod} q^e)}\begin{pmatrix}1 & u\\ 0 & q^e\end{pmatrix}.$$

且作为一个算子

$$\begin{aligned}H_NU_q^e&=q^{e(\frac{k}{2}-1)}\sum_{u(\operatorname{mod} q^e)}\begin{pmatrix}0 & -1\\ M & uM\end{pmatrix}\\&=q^{e(\frac{k}{2}-1)}H_M\sum_{u(\operatorname{mod} p^e)}\begin{pmatrix}1 & u\\ 0 & 1\end{pmatrix}.\end{aligned}$$

由于 H_N 是一个同构, 所以我们可以比较 $(H_NU_q^e)^2$ 和 $(H_NU_q^{e-1})^2$. 由上面计算得

$$(H_NU_q^e)^2=q^{e(k-2)}\sum_{u,v(\operatorname{mod} q^e)}H_M\begin{pmatrix}1 & u\\ 0 & 1\end{pmatrix}H_M\begin{pmatrix}1 & v\\ 0 & 1\end{pmatrix}.$$

我们断言

$$\sum_{\substack{u,v(\operatorname{mod} q^e)\\(u,q)=1}}H_M\begin{pmatrix}1 & u\\ 0 & 1\end{pmatrix}H_M\begin{pmatrix}1 & v\\ 0 & 1\end{pmatrix}$$

是空间 $C(N,k,\chi)$ 中的零算子. 事实上, 对一个与 q 互素的 u 以及任意的 v 和 v', 我们有

$$\begin{aligned}H_M\begin{pmatrix}1 & u\\ 0 & 1\end{pmatrix}H_M\begin{pmatrix}1 & v\\ 0 & 1\end{pmatrix}&=\begin{pmatrix}-1 & -v\\ uM & uvM-1\end{pmatrix}\\&=\begin{pmatrix}1+M(v-v') & v-v'\\ M(u(Mv'-1)-Muv+1) & 1+Mu(v'-v)\end{pmatrix}\\&\quad\times H_M\begin{pmatrix}1 & 1\\ 0 & 0\end{pmatrix}H_M\begin{pmatrix}1 & v'\\ 0 & 1\end{pmatrix}.\end{aligned}$$

特别地，在模 q^e 的意义下唯一存在一个 v', 使得

$$u(Mv'-1)-Muv+1\equiv 0 \pmod{q^e},$$

此时， $1+Mu(v'-v)\equiv u \pmod{q^e}$ 且

$$1+Mu(v'-v)\equiv 1 \pmod{M}.$$

由于 M 与 q 互素，我们总可取 $u\equiv 1 \pmod{M}$, 使得

$$1+Mu(v'-v)\equiv u \pmod{N}.$$

这样，对任意的 $f\in C(N,k,\chi)$, 有，

$$\begin{aligned} &f|_k H_M\begin{pmatrix}1 & u\\ 0 & 1\end{pmatrix}H_M\begin{pmatrix}1 & v\\ 0 & 1\end{pmatrix}\\ &=\chi(u)f|_k H_M\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}H_M\begin{pmatrix}1 & v'\\ 0 & 1\end{pmatrix}.\end{aligned}$$

由于当 v 跑遍模 q^e 的完全剩余系时， v' 亦跑遍模 q^e 的完全剩余系．于是对上面等式两边对于 v 跑遍模 q^e 的完全剩余系，以及 u 跑遍模 q^e 的缩剩余系求和可得

$$\begin{aligned} &f|_k\sum_{\substack{u,v \pmod{q^e}\\ (u,q)=1}} H_M\begin{pmatrix}1 & u\\ 0 & 1\end{pmatrix}H_M\begin{pmatrix}1 & v\\ 0 & 1\end{pmatrix}\\ &=\sum_{u}\chi(u)f|_k\sum_{v' \pmod{q^e}} H_M\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}H_M\begin{pmatrix}1 & v'\\ 0 & 1\end{pmatrix}\\ &=0.\end{aligned}$$

这是因为，由于 χ 不是一个模 M 的特征标，所以第二个和号关于 u 的求和跑遍 $(Z/NZ)^\times$ 中所有模 M 同余于 1 的元素．

总之，作为 $C(N,k,\chi)$ 上算子，我们有

$$(H_N U_q^e)^2=q^{e(k-2)}\sum_{\substack{u \pmod{q^{e-1}}\\ v \pmod{q^e}}} H_M\begin{pmatrix}1 & uq\\ 0 & 1\end{pmatrix}H_M\begin{pmatrix}1 & v\\ 0 & 1\end{pmatrix}.$$

然而，作为算子我们又知道

$$H_M\begin{pmatrix}1 & uq\\0 & 1\end{pmatrix}H_M = H_{qM}\begin{pmatrix}1 & u\\0 & 1\end{pmatrix}H_{qM}$$

及

$$H_N U_q^{e-1} = q^{(k-1)(\frac{k}{2}-1)} \sum_{u(\bmod q^{e-1})} H_{qM}\begin{pmatrix}1 & u\\0 & 1\end{pmatrix}.$$

于是

$$(H_N U_q^e)^2 = q^{e(k-2)} \sum_{\substack{u(\bmod q^{e-1})\\ v(\bmod q^e)}} H_{Mq}\begin{pmatrix}1 & u\\0 & 1\end{pmatrix} H_{Mq}\begin{pmatrix}1 & v\\0 & 1\end{pmatrix}$$

$$= q^{k-2}\, q(H_N U_q^{e-1})^2 = q^{k-1}\, (H_N U_q^{e-1})^2.$$

由此即证明了引理 5.

我们再回到对正规化新形式 $f(z) \in \mathcal{C}(N,k,\chi)$ 的 Fourier 系数 a_q 的讨论. 对 f 应用引理 5 可得

$$\lambda_f\ a_q^e \bar{a}_q^e = q^{k-1}\lambda_f a_q^{e-1}\bar{a}_q^{e-1}.$$

于是，当 $a_q \neq 0$ 时，就有

$$|a_q| = q^{(k-1)/2}.$$

如果 $e=1$, 即 $q|N$ 且 $q^2 \nmid N$, 则由引理 5 知， U_q 是 1-1 的，于是 $a_q \neq 0$. 这样剩下的只是证明在 $q^2|N$ 和 χ 不是模 N/q 的特征标的情况下， $f|_k U_q \neq 0$. 如若不然，即

$$f|_k \sum_{u(\bmod q)} \begin{pmatrix}1 & u\\0 & q\end{pmatrix} = 0.$$

那么对任意整数 v, 有

$$
\begin{aligned}
&f|_k\begin{pmatrix}1&u\\0&q\end{pmatrix}\begin{pmatrix}1&0\\vN/q&1\end{pmatrix}\\
&=f|_k\begin{pmatrix}1+vuN/q&-vu^2N/q^2\\vN&1-vuN/q\end{pmatrix}\begin{pmatrix}1&u\\0&q\end{pmatrix}\\
&=\chi(1-vuN/q)f|_k\begin{pmatrix}1&u\\0&q\end{pmatrix}\\
&=\zeta_q^{-uv}f|_k\begin{pmatrix}1&u\\0&q\end{pmatrix},
\end{aligned}
$$

其中 $\zeta_q=\chi(1-N/q)$. 由于特征标 χ 在 $1+\dfrac{N}{q}\mathbf{Z}$ 上非平凡，故 ζ_q 是一个本原 q 次单位根. 从而，对 $v=1,2,\cdots,q$, 有

$$
0=\sum_{u\,(\mathrm{mod}\,q)}\zeta_q^{vu}f|_k\begin{pmatrix}1&u\\0&q\end{pmatrix}.
$$

将上式视作变元为 $f|_k\begin{pmatrix}1&u\\0&q\end{pmatrix}$ 的 q 元一次方程组，其系数矩阵为 (ζ_q^{vu}). 利用 Vandermonde 行列式可知，该矩阵有非零行列式 $(=\pm\prod_{1\le v<u\le q}(\zeta_q^v-\zeta_q^u))$, 从而对任意的 u 有

$$
f|_k\begin{pmatrix}1&u\\0&q\end{pmatrix}=0.
$$

由此得到 $f=0$, 这与假设 f 是水平 N 的新形式矛盾.

注　在 $q^2|N$ 且 χ 不是模 N/q 的特征标时，我们事实上也证明了 U_q 是 $C(N,k,\chi)$ 上的单射，从而它是一个自同构.

总结上面的讨论，我们有下面结论.

定理 5　设 $f(z)=\sum\limits_{n=1}^{\infty}a_n e^{2\pi inz}$ 是一个权 k, 水平为 N, 特征标为 χ 的正规化新形式，p 是一个不能整除 N 的素数，q 为 N 的一个素因子，则

(1) $f|_k\mathbb{T}_p = a_p f$, $f|_k U_q = a_q f$, 以及

$$\begin{cases} a_{np} + \chi(p)p^{k-1}a_{n/p} = a_p a_n, & n \geq 1, \\ a_{nq} = a_q a_n, & n \geq 1. \end{cases}$$

从而与 f 结合的 Dirichlet 级数 $D(s,f)$ 有 Euler 积展开:

$$\begin{aligned} D(s,f) &= \sum_{n=1}^{\infty} a_n n^{-s} \\ &= \prod_{q|N}\left(1 - a_q q^{-s}\right)^{-1} \prod_{p\nmid N}\left(1 - a_p p^{-s} + \chi(p)\, p^{k-1-2s}\right)^{-1}. \end{aligned}$$

(2) 若 χ 不是一个模 N/q 的特征标, 则 $|a_q| = q^{(k-1)/2}$.

(3) 若 χ 是一个模 N/q 的特征标, 则当 $q^2|N$ 时, $a_q = 0$; 当 $q^2 \nmid N$ 时, $a_q^2 = \chi(q)q^{k-2}$, 此时, 我们有

$$f|_k W_q^N = -a_q^{-\frac{k}{2}+1} f.$$

接下来我们讨论正规化新形式的 Fourier 系数 a_p, $p \nmid N$. 由定理 4′ 知, 存在无限多个这样的素数 p, 使得 Fourier 系数 $a_p \neq 0$. 又由推论 1 知, $a_p = \chi(p)\bar{a}_p$. 设 $\mathbf{Q}(\zeta_N)$ 表示在 $\mathbf{Q}$ 上添加 N 次单位根 ζ_N 而得到的分圆域, 用 $\mathcal{O}$ 表示其整数环. 可以证明, 空间 $\mathcal{C}(\Gamma_1(N),k)$ 有一组 Fourier 系数均在 $\mathcal{O}$ 中的元素组成的基, 并且这组基也生成了由 $\mathcal{C}(\Gamma_1(N),k)$ 中所有 Fourier 系数均在 $\mathcal{O}$ 中模形式所组成的 $\mathcal{O}$ 模. 依据 Hecke 算子 $\mathbb{T}_p$ 在 Fourier 系数上的作用, 我们看出, $\mathbb{T}_p$ 的特征值一定是一个代数整数. 对于其大小, Ramanujan 首先对 $\mathrm{SL}_2(\mathbf{Z})$ 的唯一一个权 12 的正规化尖点形式

$$\Delta(z) = \sum_{n=1}^{\infty} \tau(n)\mathrm{e}^{2\pi i n z}$$

猜测 $|\tau(p)| \leq 2p^{11/2}$. Petersson 将此猜测扩充到, 对 $\mathcal{C}(\Gamma_1(N),k)$ 中 Hecke 算子 $\mathbb{T}_p$ 的任意特征值 λ_p, 均有 $|\lambda_p| \leq 2p^{\frac{k-1}{2}}$. 这就是著名的 Ramanujan-Petersson 猜想. 1969 年, Deligne[3] 证明了从 Weil 猜想可以推出 Ramanujan-Petersson 猜想对所有权 ≥ 2 的模

形式都成立．而我们在第二章中已经指出，Weil 猜想在 1973 年也被 Deligne 所证明． 1974 年， Deligne 和 Serre[6] 进一步证明了权为 1 时 Ramanujan-Petersson 猜想也成立．结合他们的工作，就有下面结论．

定理 6 (Ramanujan-Petersson 猜想)　设

$$f(z)=\sum_{n=1}^{\infty}a_n\mathrm{e}^{2\pi i\,nz}$$

是一个权 k, 级 N, 特征标为 χ 的新形式，则对任意的 $p\nmid N$, 有

$$1-a_pp^{-s}+\chi(p)p^{k-1-2s}=(1-\alpha_pp^{-s})(1-\beta_pp^{-s}),$$

其中 $|\alpha_p|=|\beta_p|=p^{(k-1)/2}$.

由定理出发可得

$$|a_p|=|\alpha_p+\beta_p|\le 2p^{\frac{k-1}{2}}.$$

故原始的 Ramanujan-Petersson 猜想可由此导出．

新形式空间 $C^+(N,k,\chi)$ 是用 Petersson 内积来定义的，从而有两个缺点：第一，定义采用的是超越的而非代数的手段；其次，这个定义并不对所有的模形式适用，这是因为 Petersson 内积并不对所有的模形式有定义．下面我们介绍一种代数的方法来刻画新形式空间 $C^+(N,k,\chi)$. 它是由 Serre[26] 首先引用来刻画由 $\Gamma_0(q)$ 上的新形式生成的空间，这里 q 为素数．

对 N 的一个正因子 M, 群 $\Gamma_0(N)$ 是群 $\Gamma_0(M)$ 的一个有限阶子群，故存在 $R_i\in\Gamma(M)$, 使得到右陪集表示

$$\Gamma_0(M)=\bigcup_i\Gamma_0(N)R_i.$$

设 χ 是模 M 的一个特征标，由空间 $\mathcal{M}(N,k,\chi)$ 到空间 $\mathcal{M}(M,k,\chi)$ 的迹算子定义为

$$\mathrm{Tr}_M^Nf=\sum_i f|_kR_i,\qquad f\in\mathcal{M}(N,k,\chi).$$

习题 19 证明：当 $f\in\mathcal{M}(N,k,\chi)$ 时，$\mathrm{Tr}_M^N f\in\mathcal{M}(M,k,\chi)$，并且迹算子的定义不依赖于陪集表示 R_i 的选取. 进一步证明迹算子映尖点形式为尖点形式.

定理 7 设 $f\in\mathcal{C}(N,k,\chi)$，则 $f\in\mathcal{C}^+(N,k,\chi)$ 的充要条件是：对 N 的任意素因子 q，若 χ 是模 N/q 的特征标，则

$$\mathrm{Tr}_{N/q}^N f=0=\mathrm{Tr}_{N/q}^N f|_k H_N.$$

证 充分性. 利用定义，我们要证明的是对 N 的所有使得 χ 为模 N/q 的特征标的素因子 q，以及对空间 $\mathcal{C}(N/q,k,\chi)$ 中任意模形式 g，一定有

$$\langle f,g\rangle=0=\langle f,g|_kB_q\rangle.$$

现设 q 是这样的一个素数，g 为这样的一个模形式. 注意到对迹算子 $\mathrm{Tr}_{N/q}^N$ 定义中的一陪集表示元 $R_i\in\Gamma(N/q)$，有

$$R_i^{-1}\Gamma(N)R_i=\Gamma(N),$$

进而 $R_i^{-1}\mathcal{D}(\Gamma(N))=\mathcal{D}(\Gamma(N))$. 于是，对任意的 i，注意到 g 的水平为 N/q，由

$$\begin{aligned}\langle f,g\rangle&=\frac{1}{[\Gamma:\Gamma(N)]}\iint\limits_{\mathcal{D}(\Gamma(N))}\delta(f,g)(z)\\&=\frac{1}{[\Gamma:\Gamma(N)]}\iint\limits_{\mathcal{D}(\Gamma(N))}\delta(f,g|_kR_i^{-1})(z)\\&=\frac{1}{[\Gamma:\Gamma(N)]}\iint\limits_{R_i^{-1}\mathcal{D}(\Gamma(N))}\delta(f,g|_kR_i^{-1})(R_iz)\\&=\frac{1}{[\Gamma:\Gamma(N)]}\iint\limits_{\mathcal{D}(\Gamma(N))}\delta(f|_kR_i,g)(z)\end{aligned}$$

结合条件 $\mathrm{Tr}_{N/q}^N f=0$，可得

$$\langle\mathrm{Tr}_{N/q}^N f,g\rangle=[\Gamma_0(N/q):\Gamma_0(N)]\langle f,g\rangle=0.$$

由假设条件 $\mathrm{Tr}_{N/q}^{N}f|_kH_N=0$, 利用上面的方法同样可以证明 $f|_kH_N$ 与 $\mathcal{C}(N/q,k,\overline{\chi})$ 中的模形式正交. 再注意到 $g|_kH_{N/q}\in\mathcal{C}(N/q,k,\overline{\chi})$, 于是就有

$$\begin{aligned}\langle f,g|_kB_d\rangle &= \langle f|_kH_N,g|_kB_q|_kH_N\rangle\\&=q^{-\frac{k}{2}}\langle f|_kH_N,g|_kH_{N/q}\rangle=0.\end{aligned}$$

从而充分性得证.

必要性. 设 q 是 N 的一个素因子且使得 χ 为模 N/q 的特征标. 于是 $\mathrm{Tr}_{N/q}^{N}f\in\mathcal{C}(N/q,k,\chi)$ 和 $\mathrm{Tr}_{N/q}^{N}f|_kH_N\in\mathcal{C}(N/q,k,\overline{\chi})$. 利用充分性部分的计算可以得到

$$\begin{aligned}\langle\mathrm{Tr}_{N/q}^{N}f,\mathrm{Tr}_{N/q}^{N}f\rangle &= [\varGamma_0(N/q):\varGamma_0(N)]\langle f,\mathrm{Tr}_{N/q}^{N}f\rangle\\&=0.\end{aligned}$$

最后一步是由于 $f\in\mathcal{C}^+(N,k,\chi)$, 而 $\mathrm{Tr}_{N/q}^{N}f\in\mathcal{C}^-(N,k,\chi)$. 这就表明 $\mathrm{Tr}_{N/q}^{N}f=0$. 由于 H_N 映 $\mathcal{C}^{\pm}(N,k,\chi)$ 为 $\mathcal{C}^{\pm}(N,k,\overline{\chi})$, 所以用同样的方法可以证明 $\mathrm{Tr}_{N/q}^{N}f|_kH_N=0$. 由此必要性部分也得到了证明.

下面我们来讨论模形式空间 $\mathcal{M}(N,k,\chi)$ 的结构. 对于同余子群 $H=\varGamma_0(N)$, $\varGamma_1(N)$, 及 $\varGamma(N)$, Hecke 构造了一个由 Eisenstein 级数组成的空间 $\mathcal{E}(H,k)$, 使得

$$M(H,k)=\mathcal{E}(H,k)\bigoplus\mathcal{C}(H,k).$$

当权 $k\geq3$ 时, $\dim_{\mathbf{C}}\mathcal{E}(H,k)$ 恰好等于 H 的尖点个数. 事实上, $\mathcal{E}(H,k)$ 有一组基, 其元限制在 H 的尖点上时, 恰好为尖点的特征函数. 这些模形式通常称为 **Eisenstein 级数**, 它们是通过二重级数来定义的; 当 $k\geq3$ 时, 这些级数是绝对收敛的. 当 $k=2$ 时, 这些二重级数是条件收敛的, 于是 Eisenstin 级数取作两个条件收敛的级数之差. 权 $k=1$ 时, Eisenstein 级数则是利用解析延拓来给出的. 尽管不存在 Eisensten 级数空间的一个 "标准" 取法来使上述分解成立, 但 Hecke 的选取是较好的, 因为该空间在 Hecke 算子作用下保持不变. 并且如果 H 是 H' 的子群, 那么 $\mathcal{E}(H',k)$ 是

$\mathcal{E}(H,k)$ 的子空间. 如同尖点形式一样, 空间 $\mathcal{E}(\Gamma_1(N),k)$ 也可分解为直和 $\bigoplus_\chi \mathcal{E}(N,k,\chi)$, 其中 χ 跑遍模 N 的所有特征标. 于是

$$\mathcal{M}(N,k,\chi) = \mathcal{E}(N,k,\chi) \bigoplus \mathcal{C}(N,k,\chi).$$

要想了解这方面更多的知识, 读者可以参阅参考文献 [10, 18, 20]. 研究表明, 对于尖点形式引入的算子对 Eisenstein 级数空间同样有意义. 当我们用迹算子方法代替 Petersson 内积方法来定义新形式后, 新形式理论同样适用于 Eisenstein 级数空间. 于是空间 $\mathcal{M}(N,k,\chi)$ 就由正规化的权 k, 特征标为 χ 的新形式及其 "提升" 生成. 当然这些模形式的水平均应为 N 的因子. 另外, 我们还需说明的是, 权 k、水平 N, 特征标为 χ 的正规化的新 Eisenstein 级数是已知的: 它们所结合的 Dirichlet 级数是两个 Dirichlet L-函数的积

$$D(s,f) = L(s,\chi_1)L(s+1-k,\chi_2),$$

其中 χ_1 和 χ_2 分别为前导子是 N_1 和 N_2 的特征标, 使得 $N = N_1N_2$ 及 $\chi = \chi_1\chi_2$. 严格地讲, $D(s,f)$ 刻画了 f 的所有非零 Fourier 系数. 我们将在下节看到, f 的首项系数恰为 $D(s,f)$ 在 $s=0$ 处残数乘以 -1.

Atkin 和 Lehner[2] 通过 $\Gamma_0(N)$ 上尖点形式的研究首先引入新形式的概念. 后来, 利用阿代尔语言, Miyake[17] 将新形式理论扩展到 $\Gamma_1(N)$ 上的模形式. 在她的博士论文 [13] 中, 李文卿解释了如何把一个关于 $\Gamma(N)$ 的模形式化为水平为 N^2, 特征标为一个模 N 的特征标的模形式, 她还给出了新形式的一些判别法, 本节的主要部分取材于 [13]. 关于 Eisenstein 级数的新形式理论则是由 Weisinger 在其博士论文 [34] 中完成的. 新形式理论同 $\mathrm{GL}_2(A_Q)$ 的表示之间的联系则分别由 Casselman[3] 和 Deligne[5] 给予了讨论.

习题 20 (1) 证明: 当 $l>2$ 时, 级数 $\sum\limits_{m,n}{}'|mz+n|^{-l}$ 在 $\mathfrak{H}$ 中的任意紧子集上一致收敛, 其中 $\sum'$ 表示求和取遍全部不等于 $(0,0)$ 的整数对

(m,n).

(2) 设 $G_k(z)=\sum\limits_{m,n}{}'(mz+n)^{-2k}$. 证明, 当 $k>1$ 时, Eisenstein 级数 $G_k(z)$ 是权 $2k$ 的关于 $\Gamma=\mathrm{SL}_2(Z)$ 的模形式, 且 $G_k(\mathrm{i}\infty)=2\zeta(2k)$. 其中 ζ 是 Riemann zeta 函数.

§4 函 数 方 程

Hecke 对模形式理论的基本贡献之一就是研究了结合于模形式的 L-函数的解析性质. 下面我们来讨论这方面的问题. 设 f 是一个权 k 的模形式,

$$\Gamma(s)=\int_0^\infty \mathrm{e}^{-t}t^{s-1}\mathrm{d}t \quad (\mathrm{Re}\, s>1)$$

是熟知的 Gamma 函数. 令

$$L(s,f)=(2\pi)^{-s}\Gamma(s)D(s,f).$$

又设 f 有 Fourier 展开

$$f(z)=\sum_{n=0}^{\infty}a_n\mathrm{e}^{2\pi\mathrm{i}nz}.$$

容易证明, 当 $n\geq 1$ 时, $a_n=O(n^k)$. 事实上, 若 f 是个尖点形式, 则由定理 6 知, 对任意的 $\varepsilon>0$, $a_n=O(n^{\frac{k-1}{2}+\varepsilon})$. 不管怎么说, Dirichlet 级数

$$D(s,f)=\sum_{n=1}^{\infty}a_nn^{-s}$$

在右半平面 $\mathrm{Re}\, s>k+1$ 中绝对收敛, 从而定义了一个全纯函数. Hecke 把 $L(s,f)$ 表示成 f 的 Mellin 变换

$$L(s,f)=\int_0^\infty t^{s-1}(f(\mathrm{i}t)-a_0)\mathrm{d}t=\int_0^\infty t^s(f(\mathrm{i}t)-a_0)\frac{\mathrm{d}t}{t}.$$

进而他研究了 $L(s,f)$ 的解析开拓和函数方程. 严格地讲, $f(\mathrm{i}t)-a_0$ 可视为正实轴 $\mathbf{R}_{>0}^\times$ 上的一个函数, 而 $\mathbf{R}_{>0}^\times$ 显然是一个乘法群.

$\mathbf{R}_{>0}^{\times}$ 上的拟特征标可以用 $t \longmapsto t^s, s \in \mathbf{C}$ 来给出，而 $\mathrm{d}t/t$ 恰为 $\mathbf{R}_{>0}^{\times}$ 上的一个 Haar 测度. 于是 f 的 Mellin 变换就可以看作函数 $f(\mathrm{i}t) - a_0$ 在 $R_{>0}^{\times}$ 上的 " Fourier 变换". 对 L-函数 $L(s,f)$ 的研究十分类似于我们在第五章中所做的对伊代尔类特征的 L-函数的讨论，于是在此我们只是简单地概述一下，请读者自己把细节补齐.

设 f 的水平为 N, 令

$$g(z) = f|_k H_N(z) = N^{-\frac{k}{2}} z^{-k} f\left(\frac{-1}{Nz}\right) = \sum_{n=0}^{\infty} b_n e^{2\pi i n z}.$$

显然 g 也是一个权 k, 水平 N 的模形式，特别地，

$$g(\mathrm{i}y) = N^{-k/2}(\mathrm{i}y)^{-k} f\left(\frac{\mathrm{i}}{Ny}\right).$$

当 $\mathrm{Re}\, s > \frac{k}{2} + 1$ 时，

$$\begin{aligned}
L(s,f) &= \int_0^1 t^{s-1}(f(\mathrm{i}t) - a_0)\mathrm{d}t + \int_1^{\infty} t^{s-1}(f(\mathrm{i}t) - a_0)\mathrm{d}t \\
&= -\frac{a_0}{s} + \int_0^1 t^s f(\mathrm{i}t)\frac{\mathrm{d}t}{t} + \int_1^{\infty} t^s(f(\mathrm{i}t) - a_0)\frac{\mathrm{d}t}{t}.
\end{aligned}$$

在第一个积分中令 $t = \frac{1}{Ny}$, 则有

$$\begin{aligned}
L(s,f) = &-\frac{a_0}{s} + \int_1^{\infty} (Ny)^{-s} f\left(\frac{\mathrm{i}}{Ny}\right)\frac{\mathrm{d}y}{y} + \int_1^{\infty} t^s(f(\mathrm{i}t) - a_0)\frac{\mathrm{d}t}{t} \\
= &-\frac{a_0}{s} + \mathrm{i}^k N^{\frac{k}{2}-s}\int_1^{\infty} y^{k-s} g(\mathrm{i}y)\frac{\mathrm{d}y}{y} \\
&+ \int_1^{\infty} t^s(f(\mathrm{i}t) - a_0)\frac{\mathrm{d}t}{t} \\
= &-\frac{a_0}{s} - \mathrm{i}^k N^{\frac{k}{2}-s}\frac{b_0}{k-s} + \mathrm{i}^k N^{\frac{k}{2}-s}\int_1^{\infty} y^{k-s}(g(\mathrm{i}y) - b_0)\frac{\mathrm{d}y}{y} \\
&+ \int_1^{\infty} t^s(f(\mathrm{i}t) - a_0)\frac{dt}{t}.
\end{aligned}$$

由于存在正常数 c, 使得当 $t \longrightarrow \infty$ 时,

$$f(\mathrm{i}t) - a_0 = O(\mathrm{e}^{-ct}) \quad 和 \quad g(\mathrm{i}t) - b_0 = O(\mathrm{e}^{-ct}),$$

这表明最后两个积分定义了两个在整个 s 平面上全纯的函数, 并且它们在任意有限宽度的垂直带中都是有界的. 由此我们就得到 $L(s,f)$ 在整个 s 平面上的解析开拓. 除在 $s=0$ 和 $s=k$ 有可能是两个单极点外, $L(s,f)$ 在整个 s 平面上全纯. 更精细一些, 由

$$\begin{aligned} &L(s,f) + \frac{a_0}{s} + \mathrm{i}^k N^{\frac{k}{2}-s} \frac{b_0}{k-s} \\ &= \mathrm{i}^k N^{\frac{k}{2}-s} \left(L(k-s,g) + \frac{b_0}{k-s} + \mathrm{i}^k N^{s-\frac{k}{2}} \frac{(-1)^k a_0}{s} \right) \end{aligned}$$

导出函数方程

$$L(s,f) = \mathrm{i}^k N^{\frac{k}{2}-s} L(k-s,g).$$

将上面讨论总结一下, 即得

定理 8 (Hecke) 设

$$f(z) = \sum_{n=0}^{\infty} a_n \mathrm{e}^{2\pi \mathrm{i} n z} \in \mathcal{M}(N,k,\chi).$$

L-函数 $L(s,f)$ 在半平面 $\mathrm{Re}\, s \gg 0$ 上是绝对收敛的. 它可以解析开拓至整个 s 平面, 且除了在 $s=0$ 和 $s=k$ 可能为单极点外处处全纯, 它在 $s=0$ 处的残数是 $-a_0$. 另外, $L(s,f)$ 在任意有限宽度的垂直带中是有界的, 并且满足函数方程

$$L(s,f) = \mathrm{i}^k N^{\frac{k}{2}-s} L(k-s, f|_k H_N).$$

特别地, 当 f 是一个水平 N 的新形式时, $f|_k H_N = \lambda_f \overline{f}$. 于是函数方程变为

$$L(s,f) = \lambda_f \mathrm{i}^k N^{\frac{k}{2}-s} L(k-s,\overline{f}) = \varepsilon(s,f) L(k-s,\overline{f}).$$

此外, 若 f 是一个尖点形式, 则 $L(s,f)$ 为一全纯函数.

注 设 f 是 $\mathcal{M}(N,k,\chi)$ 中的一个新形式, 若它的一次 Fourier 系数 $a_1 = 1$, 则它完全由 $D(s,f)$ 在所有素数处的 Euler 积以及

$L(s,f)$ 满足函数方程 $L(s,f) = C_1 N^{\frac{k}{2}-s} L(k-s,\overline{f})$ 所决定. 这里 C_1 是一个非零常数 (参见参考文献 [13, 定理 9]).

从定理 4 我们知道, 对两个有同样权和特征标的尖点新形式, 如果它们关于几乎所有的 Hecke 算子 $\mathbb{T}_p$ 有相同的特征值, 那么它们俩也应相等. 不过在那里我们要求其中一个新形式的水平可以整除另外一个. 下面我们会看到, 这个关于水平的限制条件是不需要的.

定理 9 设 $f(z) = \sum\limits_{n=1}^{\infty} a_n e^{2\pi i n z}$ 和 $g(z) = \sum\limits_{n=1}^{\infty} a'_n e^{2\pi i n z}$ 两个权 k, 特征标为 χ 的正规化尖点新形式, 它们的水平分别为 N 和 N'. 若对几乎所有的素数 p, 均有 $a_p = a'_p$, 则 $f = g$. 从而 $N = N'$.

证 这个定理可以用纯代数的方法来证明, 参见参考文献 [13]. 在这里我们将应用定理 8 来证明之. 假设 $f \neq g$, 以 K 表示使得 $a_p \neq a'_p$ 成立的那些素数 p 的积, 则

$$\frac{L(s,f)}{L(s,g)} = \frac{\prod\limits_{q|K,q|N'} (1-a'_q q^{-s}) \prod\limits_{p|K,p\nmid N'} \left(1-a'_p p^{-s}+\chi(p)p^{k-1-2s}\right)}{\prod\limits_{q|K,q|N} (1-a_q q^{-s}) \prod\limits_{p|K,p\nmid N} \left(1-a_p p^{-s}+\chi(p)p^{k-1-2s}\right)}$$

是 s 平面上的一个亚纯函数. 再利用 $L(s,f)$ 和 $L(s,g)$ 的函数方程, 我们得到下面函数方程

$$\frac{L(s,f)}{L(s,g)} = C\left(\frac{N}{N'}\right)^{\frac{k}{2}-s} \frac{L(k-s,\overline{f})}{L(k-s,\overline{g})}.$$

需要注意的是, 上式可以作为有限积的商成立, 所以并不需要再进行解析开拓. 又由于使得 $p^{-s}=1$ 成立的 s 对于 K 的不同的素因子 p 也是不同的, 所以上面函数方程可以诱导出在每个素数 $p|K$ 处的局部函数方程. 换句话说, 当 $p \nmid N$ 或 $p \nmid N'$ 时, 如果我们记

$$1-a_p p^{-s}+\chi(p)p^{k-1-2s} = (1-\alpha_p p^{-s})(1-\beta_p p^{-s})$$

和

$$1-a'_p p^{-s}+\chi(p)p^{k-1-2s}=(1-\alpha'_p p^{-s})(1-\beta'_p p^{-s})$$

那么我们可以将前述函数方程分裂成下面三种情形的局部函数方程的积:

(I) $p|K,\ p\nmid NN'$:

$$\frac{(1-\alpha'_p p^{-s})(1-\beta'_p p^{-s})}{(1-\alpha_p p^{-s})(1-\beta_p p^{-s})}=\frac{(1-\overline{\alpha'_p}p^{-k+s})(1-\overline{\beta'_p}p^{-k+s})}{(1-\overline{\alpha_p}p^{-k+s})(1-\overline{\beta_p}p^{-k+s})}\cdot c_p;$$

(II) $p|K,\ p\nmid N, p|N'$:

$$\frac{1-a'_p p^{-s}}{(1-\alpha_p p^{-s})(1-\beta_p p^{-s})}=\frac{1-\overline{a'_p}p^{-k+s}}{(1-\overline{\alpha_p}p^{-k+s})(1-\overline{\beta_p}p^{-k+s})}\cdot c_p\cdot(p^{-s})^{e(p)}$$

(情形 $p|K, p|N, p\nmid N'$ 与此情形对称, 讨论方法相同);

(III) $p|K,\ p|N,\ p|N'$:

$$\frac{1-a'_p p^{-s}}{1-a_p p^{-s}}=\frac{1-\overline{a'_p}p^{-k+s}}{1-\overline{a_p}p^{-k+s}}\cdot c_p\cdot(p^{-s})^{e(p)},$$

其中 c_p 是非零常数, $e(p)$ 是整数.

命 $x=p^{-s}$, 我们首先看到

$$(1-\alpha_p x)(1-\beta_p x)\ \text{同}\ (x-\overline{\alpha_p}p^{-k})(x-\overline{\beta_p}p^{-k})$$

没有公共零点. 这是因为由 $\overline{\alpha_p}p^{-k}=1/\beta_p$ 可以导出

$$\overline{\alpha_p}\beta_p\alpha_p\overline{\beta_p}=p^{2k};$$

而由 $\overline{\alpha_p}p^{-k}=1/\alpha_p$ 则可导出

$$|\alpha_p|=p^{k/2}.$$

不管那种情况，这些都与 Ramanujan-Petersson 猜想（定理 6）矛盾. 当然，由于 Ramanujan-Petersson 猜想的证明用到了代数几何，所以我们希望我们这里的讨论能局限于模形式中. Rankin[21] 引入了一种十分容易且有用的方法，并使用它证明了，当 n 充分大时，$a_n = O\left(n^{\frac{k-1}{2}+\frac{1}{5}}\right)$. 不管上述那种情况成立，我们均可导出，当 n 充分大时，a_{p^n} 不满足 Rankin 的估计，从而肯定了所述两个多项式没有公共零点. 这样，情形 (I) 只能在

$$a_p = \alpha_p + \beta_p = \alpha'_p + \beta'_p = a'_p$$

时成立. 而这与假设 $p|K$ 矛盾，即情形 (I) 不存在. 同样，情形 (II) 也不存在，这是因为等式两边（作为 p^{-s} 的函数）肯定有极点，而由上面讨论知两边的极点又不可能相同. 对情形 (III)，首先考虑 $a_p \neq 0$ 的情况，由定理 5 知，

$$|a_p| = p^{\frac{k}{2}-1} \text{ 或 } p^{\frac{k-1}{2}}$$

于是 $1 - a_p x$ 与 $x - \overline{a_p} p^{-k}$ 没有公共零点，从而情形 (III) 成立的条件是 $a_p = a'_p$，这显然不对，类似地，当 $a'_p \neq 0$ 时，情形 (III) 也不存在，于是

$$a_p = a'_p = 0,$$

而这照样不真. 从而假设错误，即 $f = g$.

习题 21 (1) 当 f 和 g 均为新 Eisenstein 级数时，证明定理 9 同样成立.

(2) 证明一个尖点新形式同一个新 Eisnestein 级数不可能关于几乎所有的 Hecke 算子相同的特征值.

给出一个复数列 $a_0, a_1, \cdots, a_n, \cdots$，假设它们满足某一增长条件 $a_n = O(n^c)$，那么函数

$$f(z) = \sum_{n=0}^{\infty} a_n e^{2\pi i n z}$$

在整个上半平面 $\mathfrak{H}$ 上全纯. 一个自然生成的问题是: 在什么样的条件下, f 是一个权 k, 水平 N, 特征标为 χ 的模形式? Hecke 首先就全模群的情形, 即水平 $N=1$, 特征标 χ 为平凡特征的情况进行了研究. 他指出, 如果 L-函数

$$L(s,f)=(2\pi)^{-s}\Gamma(s)D(s,f)$$

满足一定的解析性质, 那么 f 就是模形式. 具体一些讲, 我们已知, 如果 f 是关于 $\Gamma=\mathrm{SL}_2(\mathbf{Z})$ 的模形式, 那么 $f=f|_kH_1$, 于是由定理 8 可知, $L(s,f)$ 满足所述的那些解析性质和函数方程

$$L(s,f)=\mathrm{i}^kL(k-s,f).$$

反过来, 如果 $L(s,f)$ 有这样的解析性质, 将上面的推导过程反过来使用, Hecke 就证明了 f 与 $f|_kH_1$ 在半直线 $\{\mathrm{i}t:\ t>0\}$ 上相等, 再注意到 f 与 $f|_kH_1$ 都是 $\mathfrak{H}$ 上全纯函数, 于是由解析开拓知, 在 $\mathfrak{H}$ 上有 $f=f|_kH_1$. 我们知道全模群 Γ 是由平移变换 $\begin{pmatrix}1&1\\0&1\end{pmatrix}$ 和反转变换 H_1 生成的, 于是综合上面讨论就可肯定 f 为关于 Γ 的权 k 的模形式.

当 $N>1$ 时, 问题变得复杂得多. 这时仅仅有

$$f|_k\begin{pmatrix}1&1\\0&1\end{pmatrix}=f \quad 和 \quad f=f|_kH_N$$

还不足以保证 f 是个水平 N, 权 k 的模形式. 1967 年, A.Weil[33] 通过描述 f 及其他的许多扭曲 f_η 所结合的 L-函数所应满足的解析性质回答了这一问题.

给定函数 $f(z)=\sum\limits_{n=0}^{\infty}a_n\mathrm{e}^{2\pi\mathrm{i}nz}$ 和 $\mathbf{Z}$ 的特征标 η, 则 f 关于 η 的**扭曲**定义为

$$f_\eta(z)=\sum_{n=0}^{\infty}\eta(n)a_n\mathrm{e}^{2\pi\mathrm{i}nz}.$$

如果 f 是一个模形式，那么其扭曲 f_η 也是一个模形式，不过相关的参数可能会有变化. 例如，若 f 是一个权 k, 水平 N, 特征标为 χ 的正规化新形式，η 的前导子 m 与 N 互素，则容易证明，f_η 是一个权 k, 水平 Nm^2, 特征标为 $\chi\eta^2$ 的正规化新形式. 特别地，$L(s,f_\eta)$ 满足函数方程

$$L(s,f_\eta)=C_\eta(Nm^2)^{\frac{k}{2}-s}L(k-s,\overline{f}_{\overline{\eta}}),$$

其中 C_η 是一个常数,

$$C_\eta=C_1\frac{g(\eta)}{g(\overline{\eta})}\eta(-N)\chi(m),$$

这里 C_1 是 $L(s,f)$ 函数方程中的那个常数，$g(\eta)=g(\eta,\psi)$ 是 Gauss 和，加法特征标 $\psi(x)$ 取作 $\mathbf{Z}/m\mathbf{Z}$ 的标准加法特征标 $\mathrm{e}^{2\pi\mathrm{i}x/m}$. Weil[33] 指出，如果我们知道充分多 $L(s,f_\eta)$ 的解析性质，我们就可以断定 f 是一个模形式. 精确地讲，就是下面的定理.

定理 10(Weil, **模形式逆定理**) 设

$$f(z)=\sum_{n=0}^{\infty}a_n\mathrm{e}^{2\pi\mathrm{i}nz}\in\mathcal{M}(N,k,\chi);$$

又设 $f|_kH_N=C_1(-\mathrm{i})^k\overline{f}$, 则对所有前导子 $\mathrm{cond}\ \eta=m$ 与 N 互素的特征标 η, 有下面结论 $(\mathrm{A})_\eta$ 成立:

$(\mathrm{A})_\eta$ $L(s,f)$ 可以解析开拓至整个 s 平面，且除了 $s=0$ 和 $s=k$ 可能是单极点外，在其余的地方均全纯，并且在任意有限宽的垂直带中有界. 此外还满足函数方程

$$L(s,f_\eta)=C_\eta(Nm^2)^{\frac{k}{2}-s}L(k-s,\overline{f}_{\overline{\eta}}),$$

其中

$$C_\eta=C_1\frac{g(\eta)}{g(\overline{\eta})}\eta(-N)\chi(m),$$

而 $g(\eta)=g(\eta,\psi)$ 是上面所说的 Gauss 和.

反过来，设 $a_n(n=0,1,2,\cdots)$ 是复数，且存在常数 $c>0$，使得 $a_n=O(n^c)$. 又设 χ 是一个模 N 的特征标. 对于函数

$$f(z)=\sum_{n=0}^{\infty}a_n\mathrm{e}^{2\pi\mathrm{i}\,nz}$$

如果条件 $(\mathrm{A})_\eta$ 对 $\eta=1$ 和几乎所有前导子 $\mathrm{cond}\,\eta=m$ 与 N 互素的特征标 η 都成立，那么 $f\in\mathcal{M}(N,k,\chi)$，并且

$$f|_kH_N=C_1(-\mathrm{i})^k\overline{f}.$$

更进一步，若

$$D(s,f)=\sum_{n=1}^{\infty}a_nn^{-s}$$

在 $s=k-\delta$ 处绝对收敛，这里 δ 是一个小于 k 的正数，则 f 是一个尖点形式.

Weil 的这一定理在数论中有着深远的影响，它表明一个研究对象，如果其相关的 L-函数有着与模形式相关的 L-函数同样的性质，那么该研究对象必定与模形式有关. 下面我们就 Weil 定理的三个应用来说明这一点.

第一个应用是关于讨论 $\mathbf{Q}$ 上的虚二次域扩张 K 的伊代尔类特征标，此时域 K 只有一个复 Archimede 位 ∞. $\mathbf{C}^\times\cong\mathbf{R}_{>0}^\times\times S^1$ 的一个拟特征标把 $z=r\mathrm{e}^{\mathrm{i}\theta}\in\mathbf{C}^\times$ 映为 $r^{s_0}\mathrm{e}^{\mathrm{i}n\theta}$，其中 $s_0\in\mathbf{C}$，$n\in\mathbf{Z}$. 设 χ 是 $I_K/K^\times$ 的一个伊代尔类拟特征标. 如果 χ_∞ 映 $z=r\mathrm{e}^{\mathrm{i}\,\theta}$ 为 $\mathrm{e}^{\mathrm{i}\,n\theta}$，那么我们称 χ 是 k 型**代数拟特征标**. 其中 $k=|n|+1$. 注意到，一个代数拟特征标事实上就是一个特征标，所以结合一个 $I_K/K^\times$ 的 k 型代数特征标 χ 的 L-函数是

$$L(s,\chi)=\Gamma_{\mathbf{C}}\left(s+\frac{k-1}{2}\right)\prod_{\substack{v:K\text{的有限位}\\ \chi_v\text{非分歧}}}\left(1-\chi_v(\pi_v)\mathrm{N}v^{-s}\right)^{-1},$$

其中 $\Gamma_{\mathbf{C}}(s)=(2\pi)^{-s}\Gamma(s),\pi_v$ 是 K 在位 v 处完备化 K_v 中的一个

局部单值化参数. 对这样的一个特征标 χ, 定义

$$f(\chi)=\sum_{n=1}^{\infty}a_n\mathrm{e}^{2\pi\mathrm{i}\,nz}$$

使得它所结合的 Dirichlet 级数为

$$D(s,f)=\sum_{n=1}^{\infty}a_n n^{-s}=\prod_{\substack{v:K\text{的有限位}\\ \chi_v\text{非分歧}}}\left(1-\chi_v(\pi_v)N_v^{-s+\frac{k-1}{2}}\right)^{-1}.$$

从而

$$L(s,f)=\Gamma_{\mathbf{C}}(s)D(s,f)=L\left(s+\frac{1-k}{2},\chi\right).$$

Hecke 已经证明了 $L(s,\chi)$ 可以解析开拓至整个 s 平面, 除了在 $s=0$ 和 $s=1$ 处可能有单极点外处处全纯. 它还在任意有限宽的垂直带中有界, 并且满足函数方程

$$L(s,\chi)=\varepsilon(s,\chi)L(1-s,\chi^{-1}),$$

其中

$$\varepsilon\ (s,\chi)=\text{常数}\cdot N_{K/\mathbf{Q}}\ (\mathcal{D}_{K/\mathbf{Q}}\cdot\chi\ \text{的前导子})^{\frac{1}{2}-s},$$

这里 $\mathcal{D}_{K/\mathbf{Q}}$ 是扩张 $K/\mathbf{Q}$ 的共轭差积 (different). 常数可以用 Gauss 和来表示. 这一结论的证明类似于我们在第五章对函数域情形所做的讨论. 此外, 如果 χ 不是主特征标, 即 χ 不是 $|\ |^t, t\in\mathbf{C}$ 这种形式的特征标, 那么 $L(s,\chi)$ 是一个全纯函数. 从 $L(s,\chi)$ 的解析性质可以导出 $L(s,f)$ 满足条件 $(\mathrm{A})_1$. 接下来我们来讨论 f 的扭曲. $\mathbf{Z}$ 的一个 Dirichlet 特征标可以视作 $I_{\mathbf{Q}}/\mathbf{Q}^{\times}$ 的一个代数伊代尔类特征标 ξ, 此时 $\xi_\infty(r)=(\mathrm{sign}\ r)^\delta$, 其中 $\delta=0$ 或 1. 若 χ 是 $I_K/K^{\times}$ 的一个 k 型代数特征标, 则对任意 $I_{\mathbf{Q}}/\mathbf{Q}^{\times}$ 的代数伊代尔类特征标 η, $\chi\cdot\eta\circ\mathrm{N}_{K/\mathbf{Q}}$ 亦为 $I_K/K^{\times}$ 的一个 k 型代数特征标, 并且

$$L(s,f_\eta)=L\left(s+\frac{1-k}{2},\chi\cdot\eta\circ\mathrm{N}_{K/\mathbf{Q}}\right),$$

从而 $L(s,f_\eta)$ 满足条件 $(\mathrm{A})_\eta$. 由定理 10 知, $f(\chi)$ 是一个权 k, 水平 $N=\mathrm{N}_{K/\mathbf{Q}}(\mathcal{D}_{K/\mathbf{Q}}\cdot\chi$ 的前导子) 的模形式. 特别地, 如果 χ 是正则的, 即对任意 $I_{\mathbf{Q}}/\mathbf{Q}^\times$ 的伊代尔类特征标 ξ, 有

$$\chi\neq\xi\circ\mathrm{N}_{K/\mathbf{Q}},$$

那么 $f(\chi)$ 是一个尖点形式, 这是因为结合一个 Eisenstein 新形式的 L-函数是两个 Dirichlet 级数的积, 从而被一个适当的 Dirichlet 特征标扭曲后, 对应的 L-函数一定有极点.

为确定模形式 $f(\chi)$ 的特征标, 我们首先将 $I_{\mathbf{Q}}$ 嵌入到 I_K 之中. 设 v 为 $\mathbf{Q}$ 的一个位, w 为 K 的一个整除 v 的位, 则 K_w 包含 $\mathbf{Q}_v$. 如果有两个 K 的位 w 和 w' 可整除 v, 那么 $\mathbf{Q}_v$ 可以对角地嵌入到 $K_w\times K_{w'}$ 中. 以此方法, 我们把 $I_{\mathbf{Q}}$ 嵌入到 I_K 中去. 此时 χ 在 $I_{\mathbf{Q}}$ 上的限制恰为 $I_{\mathbf{Q}}/\mathbf{Q}^\times$ 的一个代数伊代尔类特征标 χ'. 接下来我们研究 $L(s,f)$ 在不整除 N 的位 p 处的 Euler 因子. 若 p 在 K 中是惯性的, 设 w 是 K 中那个唯一能整除 p 的位. 则我们可以取 $\pi_w=\pi_p$ 且 $\mathrm{N}w=p^2$. 从而该 Euler 因子为

$$\left(1-\chi_w(\pi_w)(\mathrm{N}w)^{-s+\frac{k-1}{2}}\right)^{-1}=(1-\chi_w(\pi_p)p^{k-1-2s})^{-1}.$$

若 p 在 K 中分裂, 设 w 和 w' 为 K 中整除 p 的位. 注意到 $K_w\cong\mathbf{Q}_p\cong K_{w'}$ 以及 $\mathrm{N}w=\mathrm{N}w'=p$, 故我们可以取 $\pi_w=\pi_p=\pi_{w'}$, 从而该 Euler 因子为

$$\begin{aligned}&\left(1-\chi_w(\pi_w)(\mathrm{N}w)^{-s+\frac{k-1}{2}}\right)^{-1}\left(1-\chi_{w'}(\pi_{w'})(\mathrm{N}w')^{-s+\frac{k-1}{2}}\right)^{-1}\\&=\Big(1-(\chi_w(\pi_p)+\chi_{w'}(\pi_p))p^{\frac{k-1}{2}-s}\\&\qquad+\chi_w(\pi_p)\chi_{w'}(\pi_p)\;p^{k-1-2s}\Big)^{-1}.\end{aligned}$$

取 $I_{\mathbf{Q}}/\mathbf{Q}^\times$ 的一个二次特征标 $\eta_{K/\mathbf{Q}}$ 为

$$\eta_{K/\mathbf{Q}}(x)=\begin{cases}1, & x\in\mathbf{Q}^\times\mathrm{N}_{K/\mathbf{Q}}(I_K),\\-1, & \text{其他情况}.\end{cases}$$

这样，不论 p 在 K 中是惯性的还是分裂的，Euler 因子中 p^{k-1-2s} 的系数均可写成 $(\chi'\eta_{K/\mathbf{Q}})(\pi_p)$. 用阿代尔观点来说，这就是说 $f(\chi)$ 的特征标恰为 $\chi'\eta_{K/\mathbf{Q}}$. 总结上述讨论，我们有

定理 11 设 χ 是 $I_K/K^\times$ 的 k 型代数伊代尔类特征标，则存在一个权 k, 水平 $N=\mathrm{N}_{K/\mathbf{Q}}(\mathcal{D}_{K/\mathbf{Q}}\cdot\chi$ 的前导子), 特征标为 $\chi'\eta_{K/\mathbf{Q}}$ 的模形式 $f(\chi)$, 其中 χ' 是 χ 在 $I_\mathbf{Q}$ 上的限制，使得

$$L(s,f)=L\left(s+\frac{1-k}{2},\chi\right).$$

进一步，如果 χ 还是正则的，那么 $f(\chi)$ 是尖点形式，同时，$f(\chi)$ 还是一个水平 N 的新形式.

最后一个关于 $f(\chi)$ 为新形式的结论虽然没有在前面提及，但由前面的讨论可以很容易推出这一点，我们留给读者作为练习.

Weil 定理的第二个应用是关于 Galois 群 $G=\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ 的不可约表示. 从第六章 §1 中的讨论我们已经知道 G 的每个有限维 (复) 不可约表示 ρ 都结合了一个 Artin L-函数 $L(s,\rho)$. 当 ρ 是一维时，存在 $I_\mathbf{Q}/\mathbf{Q}^\times$ 的一个有限阶伊代尔类特征标 χ, 使得

$$L(s,\rho)=L(s,\chi).$$

于是利用前面提到的 Hecke 关于 $L(s,\chi)$ 的工作，从而得知 $L(s,\rho)$ 的性质. 当 ρ 是一个次数 ≥ 2 的不可约表示时，在 s 的某一右半平面上 $L(s,\rho)$ 是有定义的并且还是全纯的. 类似于一维的情况，Artin 猜测说："$L(s,\rho)$ 也可以开拓成整个 s 平面上的全纯函数，并且在每个有限宽的垂直带中有界，此外还满足函数方程

$$L(s,\rho)=\varepsilon(s,\rho)L(1-s,\check{\rho}),$$

这里 $\check{\rho}$ 是 ρ 的逆步表示." 我们知道，对 G 的任何一个特征标 χ, 即 G 的一个次数为 1 的表示，$\rho\bigotimes\chi$ 是一个与 ρ 同次的不可约表示，从而由 Artin 猜想判断，$L(s,\rho\bigotimes\chi)$ 与 $L(s,\rho)$ 应有相同的解析性质，只是函数方程变为

$$L(s,\rho\bigotimes\chi)=\varepsilon(s,\rho\bigotimes\chi)L(1-s,\check{\rho}\bigotimes\chi^{-1}).$$

利用 Brauer 的一个定理，$L(s,\rho)$ 总可写成 $L(s,\chi_i)^{a_i}$ 的有限乘积，其中 χ_i 为 G 的特征标，$a_i \in \mathbf{Z}$. 从而 Artin 猜想除了将全纯延拓改为 "$L(s,\rho)$ 可解析开拓为全平面上的一个亚纯函数" 之外都是成立的.

下面我们集中讨论 ρ 是 G 的次数为 2 的不可约表示时的情况. 利用定义，$L(s,\rho)$ 总可写成局部 L 因子 $L_v(s,\rho)$ 的积

$$L(s,\rho) = \prod_v L_v(s,\rho),$$

这里 v 过 $\mathbf{Q}$ 的所有位. 按照其复共轭的行列式是 1 还是 -1, 我们称表示 ρ 是偶的或是奇的. 在 Archimede 位 ∞ 处的 L 因子 $L_\infty(s,\rho)$ 同 ρ 的奇偶性有关. 当 ρ 是奇的时，

$$L_\infty(s,\rho) = \Gamma_{\mathbf{C}}(s) = (2\pi)^{-s}\Gamma(s);$$

而当 ρ 为偶的时，按照复共轭的作用是恒等映射还是负恒等映射，$L(s,\rho)$ 分别定义为 $\Gamma_{\mathbf{R}}(s)^2$ 或 $\Gamma_{\mathbf{R}}(s+1)^2$, 其中 $\Gamma_{\mathbf{R}}(2s) = \pi^{-s}\Gamma(s)$ (参见参考文献 [31]). 在有限位 v 处，L 因子 $L_v(s,\rho)$ 或者是 1, 或着是 $(1 - a_v \mathrm{N}v^{-s})^{-1}$, 或者是 $(1 - \mathrm{Tr}\,\rho(\mathrm{Frob}_v)\ \mathrm{N}v^{-s} + (\det\rho)(\mathrm{Frob}_v)\,\mathrm{N}v^{-2s})^{-1}$; 且对几乎所有的位 v,

$$L_v(s,\rho) = (1 - \mathrm{Tr}\,\rho(\mathrm{Frob}_v)\mathrm{N}v^{-s} + (\det\rho)(\mathrm{Frob}_v)\mathrm{N}v^{-2s})^{-1}.$$

注意到行列式 $\det\rho$ 是 G 的一维表示，从而可视为 $I_{\mathbf{Q}}/\mathbf{Q}^\times$ 的一个代数伊代尔类特征标，或是 $\mathbf{Z}$ 的一个 Dirichlet 特征标. 于是，结合一个 G 的二次奇不可约表示 ρ 的 Artin L-函数 $L(s,\rho)$ 同结合一个模形式的 L-函数有相同的形式. 如果 Artin 猜想正确的话，那么就存在一个权为 1, 特征标为 $\det\rho$ 的尖点形式 $f(\rho)$, 使得

$$L(s,f(\rho)) = L(s,\rho).$$

事实上，由函数方程可以看出 $f(\rho)$ 是一个水平等于 ρ 的 Artin 前导子的新形式. 反过来，Deligne 和 Serre[5] 已经证明了，对每个权 1, 水平 N, 特征标为 χ 的新形式 f, 总存在一个 G 的二次奇不

可约表示 ρ, 使得

$$L(s,\rho) = L(s,f).$$

于是对这样的 ρ, Artin 猜想成立. 因此, 对 G 的二次奇不可约表示, Artin 猜想即等价于这样表示均可以由权 1 的新形式产生. 对于 G 的二次偶不可约表示呢? 我们只需将上述结论中的"奇"换成"偶", "新形式"换成" Maass 新形式"就可以了. Maass 形式与模形式十分相似, 它同样也有新形式理论, 只不过 Maass 形式是实解析的而不像模形式那样是全纯的. 关于 Maass 形式的介绍可以参见 Maass 的著作 [14].

Weil 定理的第三个应用是关于椭圆曲线的, 设 E 是一条定义在 $\mathbf{Q}$ 上的椭圆曲线, 它在 $\mathbf{Q}$ 上有一个极小模, 称为 **Néron 模型**. 在有限位 p 处, E 模 p 是一条定义在有限域 $\mathbf{Z}/p\mathbf{Z}$ 上的曲线. 注意, 对几乎所有的 p, 这样的曲线仍是椭圆曲线. 当 E 模 p 是一条椭圆曲线时, 我们可以像在第二章中那样定义它的 zeta 函数, 并如同第五章中那样研究这个 zeta 函数的性质. 如果以 N_p 表示它的 $\mathbf{Z}/p\mathbf{Z}$ 有理点个数, 则这个 zeta 函数可以写成

$$\frac{1 - a_p p^{-s} + p^{1-2s}}{(1-p^{-s})(1-p^{1-s})},$$

其中 $a_p = 1 + p - N_p$. 此时, 定义

$$L_p(s,E) = (1 - a_p p^{-s} + p^{1-2s})^{-1}.$$

当 E 模 p 不是一条椭圆曲线时, 此时有几种可能性: 第一, 它有一个具有两条有理斜率切线的结点; 第二, 它有一个有两条无理斜率切线的结点 (此时, 我们称 E 在 p 处有一个**乘法约化**); 第三, 它有一个尖点 (此时, 称 E 在 p 处有一个**加法约化**), 它在 p 处的局部 L 因子 $L_p(s,E)$ 分别取作

$$(1-p^{-s})^{-1}, \quad (1+p^{-s})^{-1} \quad 和 \quad 1.$$

又存在一个正整数 N, 使得 $p|N$ 的充要条件是 E 模 p 不是一条椭圆曲线, 这个数 N 反映了 E 模 p 的一些几何性质, 我们称它为 E

的前导子 (conductor). 所以结合 E 的整体 L-函数可定义为

$$\begin{aligned}L(s,E) &= \Gamma_{\mathbf{C}}(s) \prod_{p:\text{素数}} L_p(s,E) \\ &= (2\pi)^{-s}\Gamma(s)\prod_{q|N}(1-a_q q^{-s})^{-1}\prod_{p\nmid N}(1-a_p p^{-s}+p^{1-2s})^{-1}.\end{aligned}$$

局部 L 因子的乘积 $\prod_p L_p(s,E)=\zeta(s,E)=\sum_{n=1}^{\infty} a_n n^{-s}$ 又称为 E 的 **Hasse-Weil zeta 函数**, Hasse 猜测了它的解析性质.

Hasse 猜想　设 E 为 $\mathbf{Q}$ 上的椭圆曲线, η 是任意一个 Dirichlet 特征标, 则 $L(s,E)$ 及它被 η 的扭曲 $L(s,E,\eta)$ 均可全纯开拓至整个 s 平面, 它们在任意有限宽的垂直带中有界, 并且满足函数方程

$$L(s,E)=\varepsilon(s,E)L(2-s,E),$$

$$L(s,E,\eta)=\varepsilon(s,E,\eta)L(2-s,E,\overline{\eta}),$$

这里 $\varepsilon(s,E)=c_1N^{1-s}$, 其中 N 为 E 的前导子, c_1 是一非零常数. 当 η 的前导子与 N 互素时, $\varepsilon(s,E,\eta)$ 与 $\varepsilon(s,E)$ 的关系可以由 $(\mathrm{A})_\eta$ 给出.

按定理 10 的观点, Hasse 猜想事实上是说, 任意给定一条 $\mathbf{Q}$ 上的椭圆曲线, 总可找到一个权 2, 水平 N, 特征标平凡的新形式 $f(E)$, 使得 $L(s,f(E))=L(s,E)$.

下面设 g 是一个关于 $\Gamma_0(N)$ 的权 2 的非零尖点形式, 从而 $g(z)\mathrm{d}z$ 是模曲线 $X_0(N)=\widehat{\mathfrak{H}/\Gamma_0}(N)$ 上的一个全纯微分形式. 这个微分形式通过将 1-闭链 γ 映为积分

$$\int_\gamma g(z)\mathrm{d}z$$

而定义了一个从 $H_1(X_0(N),\mathbf{Z})$ 到 $\mathbf{C}$ 的同态. 它的像是 $\mathbf{C}$ 中秩为 2 的格, 记作 L_g, 并称之为 $g(z)\mathrm{d}z$ 的周期格. $E_g=\mathbf{C}/L_g$ 是一条椭圆曲线, 于是我们就得到了一个从 $X_0(N)$ 到 E_g 的映射 ϕ, 它是

由一个从 $\mathfrak{H}$ 到 $\mathbf{C}$, 将 $\tau \in \mathfrak{H}$ 映为

$$\int_{i\infty}^{\tau} g(z)\mathrm{d}z$$

的映射诱导出来的. 显然, $\phi(i\infty) = 0 \in E_g$.

设 E 是 $\mathbf{Q}$ 上一条椭圆曲线, 它在 $\mathbf{Z}$ 上的 Néron 模由方程

$$y^2 = f(x) = 4x^3 + g_2 x + g_3$$

给出. 设 ω 是微分形式

$$\frac{\mathrm{d}\,x}{y} = \frac{2\mathrm{d}\,y}{f'(x)},$$

它生成了 E 上的全纯微分形式空间. 如果 E 表示为 $\mathbf{C}/L$, 其中 $L = \{1, z\}$, 那么 ω 即为 $\mathrm{d}z$. 如果存在一个映 $i\infty$ 为 0 的态射

$$\psi : X_0(N) \longrightarrow E,$$

那么, 由 Eichler-Shimura 和 Igusa 建立的关于模对应的同余关系 (Eichler-Shimura 关系) 知, 微分形式的拉回 $\psi^*\omega$ 恰好等于 $c \cdot h(z)\mathrm{d}z$. 其中 $c \in \mathbf{Q}^{\times}$, $h(z)$ 是 $\mathcal{C}(\Gamma_0(N), 2)$ 中的正规化新形式, 对任意的 $p \nmid N$, $h(z)$ 关于 Hecke 算子 $\mathbb{T}_p$ 的特征值正好是 $1 + p - N_p$. 换句话说, 除了有限多个可能的因子之外, h 的 L-函数与 $L(s, E)$ 相等.

让我们把上面的讨论总结一下, 对一个 $\mathbf{Q}$ 上的椭圆曲线 E, 如果 Hasse 猜想成立, 我们总可以找到一个权 2 的尖点新形式

$$f = f(E) \in \mathcal{C}^+(\Gamma_0(N), 2),$$

使得 $L(s, f) = L(s, E)$. 而对这样的模形式 f, 我们又可构造一条 $\mathbf{Q}$ 上的椭圆曲线 E_f, 使得存在一个映 $i\infty$ 为 0 的态射

$$\psi : X_0(N) \longrightarrow E_f.$$

取 E_f 上的典范微分形式 ω, 我们又可得到一个权 2 的尖点新形式 $h \in \mathcal{C}^+(\Gamma_0(N), 2)$, 它与 f 关于所有的 Hecke 算子 $\mathbb{T}_p (p \nmid N)$ 的特

征值相同，从而

$$h = f, \quad L(s, E) = L(s, E_f).$$

由被 Faltings[8] 所证明的 Shafarevich 猜想知，E 和 E_f 是同源的 (isogeneous)(亦可参见参考文献 [29] 第七章中的讨论). 于是存在一个从 $X_0(N)$ 到 E 的态射，它映 $i\infty$ 为 0，且使得 E 上 Néron 微分形式 ω_E 的拉回 $\psi^*(\omega_E)$ 是 $C(\Gamma_0(N), 2)$ 中一个新形式的非零有理倍数. 具有这样性质的椭圆曲线称为 **Weil 曲线**. 上面的讨论表明：由 Hasse 猜想导出下面的猜想.

Taniyama-Shimura 猜想 任何一条 **Q** 上的椭圆曲线均为 Weil 曲线.

反过来，对椭圆曲线 E，若 Taniyama-Shimura 猜想成立，则存在尖点新形式 f，使得

$$L(s, E) = L(s, f),$$

从而 Hasse 猜想也成立. 这就是说， Taniyama-Shimura 猜想与 Hasse 猜想等价. 这方面更深入的讨论可以参阅参考文献 [15, 27, 30].

K. Ribet[21] 证明了由 Taniyama-Shimura 猜想可以导出著名的 **Fermat 大定理**：“对不小于 3 的正整数 n，方程 $x^n + y^n = z^n$ 只有平凡的整数解.” 最近， A. Wiles 和 R. Taylor[32,35] 证明了 Taniyama-Shimura 猜想对 Q 上的半稳定的椭圆曲线成立. 而将此结论再结合 Ribet 的结果足以导出 Fermat 大定理的正确. 有关这方面的讨论可见参考文献 [23,24,25].

参 考 文 献

[1] A. N. Andrianov, *Quadratic Forms and Hecke Operators*, Springer-Verlag, Berlin, Heidelberg, New York, 1987.

[2] A. O. L. Atkin and J. Lehner, *Hecke operators on $\Gamma_0(m)$*, Math. Ann., **185** (1970), 134～160.

[3] W. Casselman, *On some results of Atkin and Lehner*, Math. Ann., **201** (1973), 301~314.

[4] P. Deligne, *Formes Modulaires et Représentations l-adiques*, In: Séminaire Bourbaki, vol. 1968/69, Lecture Notes in Math., 179, Springer-Verlag, Berlin, Heidelberg, New York, 1973, 55~105.

[5] P. Deligne, *Formes Modulaires et Représentations de* GL(2). In: Modular Functions of One Variable II, Lecture Notes in Math., 349, Springer-Verlag, Berlin, Heidelberg, New York, 1973, 55~105.

[6] P. Deligne and J. P. Serre, *Formes modulaires de poids* 1. Ann. Sci. E. N. S., **7** (1974), 507~530.

[7] P. Degligne and W. Kuyk, *Modular Functions of One Variable*, I, II, Proceedings of the International Summer School on "Modular functions of one variable and arithmetical applications" Univ. of Antwerp, RUCA, July 17-Aug. 3, 1972; Lecture Notes in Math., 320, 349, Springer-Verlag, Berlin, Heidlberg, New York, 1973.

[8] G. Faltings, *Endlichkeitssatze für abelsche Varietaten über Zahlkorpern*, Invent. Math., **73** (1983), 340~366; *Erratum*, ibid., **75** (1984), 381.

[9] R. C. Gunning, *Lectures on Modular Forms*, Princeton University Press, Princeton, N. J., 1962.

[10] E. Hecke, *Mathematische Werke*, Gottingen: Vandenhoeck und Ruprecht, 1959.

[11] D. Husemöller, *Elliptic Curves*, GTM 111, Springer-Verlag, Berlin, Heidelberg, New York, 1987.

[12] S. Lang, *Introduction to Modular Forms*, Springer-Verlag, Berlin, Heideberg, New York, 1976.

[13] W.-C. W. Li(李文卿), *Newforms and functional equations*, Math. Ann., **212** (1975), 285~315.

[14] H. Maass, *Lectures on Modular Functions of One Complex Variable*, Tata Institute of Fundamental Research, Bombay, 1964.

[15] B. Mazur, *Courbes elliptiques et symboles modulaires*, In: Seminaire Bourbaki vol. 1971/72, Lecture Notes in Math., 317, Springer-Verlag, Berlin, Heidelberg, New York, 1973.

[16] T. Miyake, *Modular Forms*, Springer-Verlag. Berlin, Heideberg, New York, 1989.

[17] T. Miyake, *On automorphic forms on* GL_2 *and Hecke operators*, Annals of Math., **94** (1971), 174~189.

[18] A.P. Ogg, *Modular Forms and Dirichlet Series*, Benjamin. New York, Amsterdam, 1969.

[19] A.P. Ogg, *On the eigenvalues of Hecke operators*, Math. Ann., **179** (1969), 101~108.

[20] R. Rankin, *Modular Forms and Functions*, Cambridge Univ. Press, Cambridge, 1977.

[21] R. Rankin, *Contributions to the theory of Ramanujan's function* $\tau(n)$ *and similar arithmetical functions*, II, Proc. Camb. Phil. Soc., **35** (1939), 357~372.

[22] K. Ribet, *On modular representations of* $\mathrm{Gal}(\overline{Q}/Q)$ *arising from modular forms*, Invent. Math., **100** (1990), 431~476.

[23] K. Ribet, *Galois representations and modular forms*, Bull. Amer. Math. Soc., to appear.

[24] K. Ribet and B. Hayes, *Fermat's last theorem and modular arithmetic*, American Scientist, Scientific Research Society, March-April (1994), 144~156.

[25] K. Rubin and A. Silverberg, *A report on Wiles' Cambridge lectures*, Bull. Amer. Math. Soc., **31** (1994), 15~38.

[26] J. P. Serre. *A Course in Arithmetic*, GTM 7, Springer-Verlag, Berlin, Heidelberg, New York, 1973.

[27] J. P. Serre, *Abelian l-Adic Representations and Elliptic Curves*, Benjamin, New York, Amsterdam, 1968.

[28] J. P. Serre, *Formes modulaires et fonctions zêta p-adiques*, In: Mod-

ular Functions of One Variable III, Lecture Notes in Math., 350, Springer-Verlag, Berlin, Heidelberg, New York, 1973, 191~268.

[29] G. Shimura, *Introduction to the Arithmetic Theory of Automorphic Functions*, Iwanami Shoten and Princeton Univ. Press , 1971.

[30] H. P. F. Swinnerton-Dyer and B. J. Birch, *Elliptic curves and modular functions*, In: Modular Functions of One Variable IV, B. J. Birch and W. Kuyk edited, Lecture Notes in Math., 476, Springer-Verlag, Berlin, Heidelberg, New York, 1975, 2~32.

[31] J. Tate, *Fourier analysis in number fields and Hecke's zeta-functions*, In: Algebraic Number Theory, J.W.S. Cassels and A. Fröhlich edited, Thompson, Washington D. C., 1967, 305~347, republished by Academic Press, London, 1989.

[32] R. Taylor and A. Wiles, *Ring theoretic properties of certain Hecke algebra*, Ann. of Math., to appear.

[33] A. Weil, *Uber die Bestimmung dirichletsher reihen durch funktionalgleichungen*, Math. Ann., **168** (1967), 149~156.

[34] J. Weisinger, *Some results on classical Eisenstein series and modular forms over function fields*, Thesis, Harvard University, Cambridge, Mass. 1977.

[35] A. Wiles, *Modular elliptic curves and Fermat's last theorem*, Ann. of Math., to appear.

第七章附录：　模形式的构造

读者通过正文中已经对模形式的经典理论有了一个比较完整的了解．在这个附录中，我们将借助于一些典型的例子，让大家能对模形式有一个更具体的认识．

1．全模群上的模形式

在这一节里我们将在全模群 $\Gamma(1)$ 上讨论．由于 $-I \in \Gamma(1)$，所以对一个全模群上权 k 的模形式 f，利用关系

$$f|_k(-I) = f(z) = (-1)^k f(z)$$

可知：当 k 是奇数时，$f = 0$．因此我们只需讨论权为偶整数的模形式．

从习题 20 中我们已经知道，当 $k > 1$ 时，级数

$$\sum_{m,n}{}' \frac{1}{|mz+n|^{2k}}$$

是收敛的．进而可以证明函数

$$G_k(z) = \sum_{n,m}{}' (mz+n)^{-2k}, \qquad k > 1$$

是全模群 $\Gamma(1)$ 的权为 $2k$ 的 (全纯) 模形式．它在 $i\infty$ 处的值为 $2\zeta(2k)$，其中 ζ 是 Riemann zeta 函数．这个函数我们称之为 $\Gamma(1)$ 的 **Eisenstein 级数**．

权最小的 Eisenstein 级数是 G_2 和 G_3，它们分别是权为 4 和 6 的模形式．由于椭圆曲线理论的原因，通常我们分别用

$$g_2 = 60G_2 \quad \text{和} \quad g_3 = 140G_3$$

来代替 G_2 和 G_3. 现在我们来看看 Eisenstein 级数与椭圆曲线的关系.

对 $z \in \mathfrak{H}$, 令

$$\mathfrak{E}(\tau, z) = \frac{1}{\tau^2} + \sum_{m,n}{}' \left(\frac{1}{(\tau - mz - n)^2} - \frac{1}{(mz + n)^2} \right), \quad \tau \in \mathbf{C}$$

是它对应的 Weierstrass 函数. 我们把 $\mathfrak{E}(\tau, z)$ 按 τ 作 Laurent 展开

$$\mathfrak{E}(\tau, z) = \frac{1}{\tau^2} + \sum_{k=2}^{\infty} (2k-1) G_k(z) \tau^{2k-2}.$$

如果命 $x = \mathfrak{E}(\tau, z)$, $y = \mathfrak{E}'_\tau(\tau, z)$, 则我们有

$$y^2 = 4x^3 - g_2 x - g_3, \tag{a.1}$$

其中 $g_2 = 60G_2$, $g_3 = 140G_3$, 如上所示. 可以证明在射影平面中由方程 (a.1) 所定义的三次曲线同构于椭圆曲线 $\mathbf{C}/L$, 这里 L 是由 1 和 z 生成的 $\mathbf{C}$ 上的格. 椭圆曲线 $\mathbf{C}/L$ 是非奇异曲线, 故其判别式不为 0. 由于 $g_2^3 - 27g_3^2$ 与多项式 $4x^3 - g_2 x - g_3$ 的判别式只相差一个常数因子, 从而可得函数

$$\Delta = (2\pi)^{-12}(g_2^3 - 27g_3^2) \neq 0.$$

利用已知的值 $\zeta(4)$ 和 $\zeta(6)$ 可知

$$g_2(\mathrm{i}\infty) = \frac{4}{3}\pi^4, \quad g_3(\mathrm{i}\infty) = \frac{8}{27}\pi^6.$$

进而有 $\Delta(\mathrm{i}\infty) = 0$, 即 Δ 是一个权为 12 的尖点形式.

由于 $\Gamma(1)$ 只有一个尖点的 ∞, 所以我们有

$$\mathcal{M}_{2k}(\Gamma(1)) = \mathbf{C}G_k + \mathcal{C}_{2k}(\Gamma(1)). \tag{a.2}$$

为了了解模形式空间更精密的结构, 我们引入一个公式.

若 f 是 $\mathfrak{H}$ 上不恒为 0 的亚纯函数, p 是 $\mathfrak{H}$ 中一点. 我们用 $v_p(f)$ 表示 f 在 p 处的阶, 即是使 $f(z)(z-p)^{-n}$ 在 p 处全纯且不为 0 的整数 n.

对一个权为 $2k$ 的 (亚纯) 模形式 f, 关系式

$$f(z)=(cz+d)^{-2k}f\left(\frac{az+b}{cz+d}\right)$$

表明, 当 $\gamma\in\Gamma(1)$ 时, $v_p(f)=v_{\gamma(p)}(f)$, 即 $v_p(f)$ 只依赖于 p 在 $\mathfrak{H}/\Gamma(1)$ 中的像. 此外我们定义 $v_\infty(f)$ 为 f 在 $i\infty$ 的 Fourier 展开式中第一个不为 0 的项的次数. 关于 $v_p(f)$ 有下面公式:

定理 1　设 f 是 $\Gamma(1)$ 的权为 $2k$ 的模形式, 则

$$v_\infty(f)+\frac{1}{2}v_i(f)+\frac{1}{3}v_\rho(f)+\sum_{\substack{p\in\mathfrak{H}/G\\ p\neq \mathrm{i},\rho}}v_p(f)=\frac{k}{12},\tag{a.3}$$

其中 $\mathrm{i}=\sqrt{-1}$, $\rho=\mathrm{e}^{2\pi\mathrm{i}/6}$.

首先, 由于 f 在 $\Gamma(1)$ 的基本区域只有有限多个零点和极点, 因此, (a.3) 式是有意义的. 简单地讲, 定理的证明可以通过对 $\dfrac{1}{2\pi\mathrm{i}}\dfrac{\mathrm{d}f}{f}$ 在基本区域的边界上积分并结合残数定理得到. 由于 f 在基本区域的边界上可能会有极点或零点, 所以积分路径 $\mathcal{L}$ 需要按图 4 处

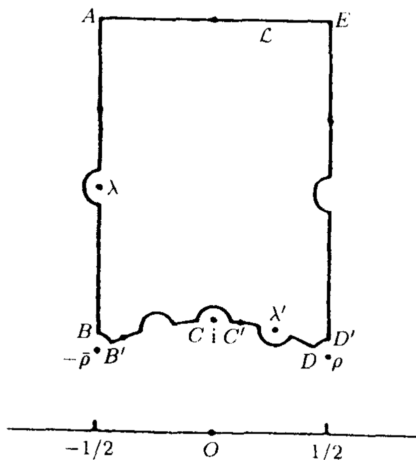


图　4

理一下：利用弧 $\overset{\frown}{EA}, \overset{\frown}{BB'}, \overset{\frown}{CC'}$ 和 $\overset{\frown}{DD'}$ 将 $\infty, -\overline{\rho}, \mathrm{i}$ 和 ρ 排除在外，如果在基本区域的边界上还有极点或零点 λ, λ', 则可以将围道在 λ 和 $\lambda+1$, λ' 和 $-1/\lambda'$ 临近处稍加变化 (如图所示，绕 $\lambda+1$ 的圆弧是用绕 λ 的圆弧平移得到，绕 $-1/\lambda'$ 的圆弧是用绕 λ' 的圆弧反转得到); 如果 f 在边界上有多个零点或极点，可类似地处理. 这样我们可以要求围道内部包含了除 ∞, i 和 ρ 以外 f 的所有零点和极点的代表元，其中也没有互相等价的. 利用残数定理可得

$$\frac{1}{2\pi\mathrm{i}}\int_{\mathcal{L}}\frac{\mathrm{d}f}{f}=\sum_{\substack{p\in\mathfrak{H}/G\\ p\neq\mathrm{i},\rho}}v_p(f).$$

此外,

$$\frac{1}{2\pi\mathrm{i}}\int_{E}^{A}\frac{\mathrm{d}f}{f}=-v_\infty(f);$$

当圆弧 $\overset{\frown}{BB'}$ 的半径趋于 0 时,

$$\frac{1}{2\pi\mathrm{i}}\int_{B}^{B'}\frac{\mathrm{d}f}{f}=-\frac{1}{6}v_\rho(f);$$

当圆弧 $\overset{\frown}{DD'}$ 的半径趋于 0 时,

$$\frac{1}{2\pi\mathrm{i}}\int_{D}^{D'}\frac{\mathrm{d}f}{f}=-\frac{1}{6}v_\rho(f);$$

当圆弧 $\overset{\frown}{CC'}$ 的半径趋于 0 时,

$$\frac{1}{2\pi\mathrm{i}}\int_{C}^{C'}\frac{\mathrm{d}f}{f}=-\frac{1}{2}v_i(f).$$

在 $\overset{\frown}{B'C}$ 与 $\overset{\frown}{C'D}$ 上的积分之和趋于 $k/12$, 而在其余边界上的积分正好抵消为 0. 综合上面讨论即得 (a.3) 式.

利用定理 1 和 (a.2) 式，我们可以很容易地推出下面的定理.

定理 2 对全模群上的模形式，我们有下面结论:

(1) $\mathcal{M}_0(\Gamma(1))=\mathbf{C}$;

(2) 若 $k<0$ 或 $k=1$, $\mathcal{M}_{2k}(\Gamma(1))=0$;

(3) 若 $k=2,3,4,5,7$, $\mathcal{M}_{2k}(\Gamma(1))=\mathbf{C}G_k$;

$$(4)\ \mathcal{C}_{2k}(\Gamma(1))=\begin{cases}0, & k<6 \text{ 或 } k=7;\\ \mathbf{C}\Delta, & k=6;\\ \Delta\mathcal{M}_{2k-12}(\Gamma(1)), & k>7.\end{cases}$$

作为定理的推论，我们有

推论 1　全模群上模形式空间的维数为

$$\dim \mathcal{M}_{2k}(\Gamma(1))=\begin{cases}\left[\dfrac{k}{6}\right], & \text{若 } k\equiv 1 \pmod 6;\\ \left[\dfrac{k}{6}\right]+1, & \text{若 } k\not\equiv 1 \pmod 6.\end{cases}$$

推论 2　全模群上权 $2k(k>1)$ 的模形式均可以写成

$$G_2(z)^aG_3(z)^b,\quad 2a+3b=k$$

这种形式函数的线性组合. 事实上，集合

$$\{G_2(z)^aG_3(z)^b : a,b\in\mathbf{Z}, 2a+3b=k, a\geq 0, b\geq 0\}$$

构成了空间 $\mathcal{M}_{2k}(\Gamma(1))$ 的一组基.

注　可以证明 G_2 和 G_3 是代数无关的. 如果我们将诸空间 $\mathcal{M}_{2k}$ 直和，则可得到一个分次代数

$$\mathcal{M}=\bigoplus_{k=0}^{\infty}\mathcal{M}_{2k}.$$

一个将 X 映为 G_2, Y 映为 G_3 的映射 $\epsilon:\mathbf{C}[X,Y]\longrightarrow\mathcal{M}$ 建立了多项式代数 $\mathbf{C}[X,Y]$ 与分次代数 $\mathcal{M}$ 之间的同构.

关于函数 Δ, 可以证明它有下面形式的 Euler 积:

$$\Delta(z)=q\prod_{n=1}^{\infty}(1-q^n)^{24},\qquad q=\mathrm{e}^{2\pi\mathrm{i}z}.$$

证明这个等式的方法很多，其中的一个想法是证明函数

$$F(z) = q\prod_{n=1}^{\infty}(1-q^n)^{24}, \qquad q = \mathrm{e}^{2\pi \mathrm{i} z}$$

是一个权为 12 的尖点形式. 这样由于 $\mathcal{C}_{12}(\Gamma(1))$ 的维数是 1, 于是 F 与 Δ 只能相差一个常数, 从而通过比较首项 Fourier 系数即得 (细节可参阅参考文献 [26] 等有关文献). 如果我们用 $\tau(n)$ 表示 $\Delta(z)$ 的第 n 项 Fourier 系数, 则有

$$\Delta(z) = \sum_{n=1}^{\infty}\tau(n)q^n = q\prod_{n=1}^{\infty}(1-q^n)^{24}, \qquad q = \mathrm{e}^{2\pi \mathrm{i} z}.$$

函数 $n \longmapsto \tau(n)$ 称为 **Ramanujan函数**. Ramanujan 首先对它进行了研究, 并提出了下列一些猜想:

(I) 若 n, m 互素, 则 $\tau(nm) = \tau(n)\tau(m)$;

(II) 设 p 为素数, $n > 1$, 则

$$\tau(p^{n+1}) = \tau(p)\tau(p^n) - p^{11}\tau(p^{n-1});$$

(III) 对任意素数 p, $|\tau(p)| < 2p^{11/2}$.

猜想 (I) 和 (II) 是由 Mordell 首先证明的. 如果从模形式的观点来看, 猜想 (I), (II) 不过是说 Δ 是所有 Hecke 算子的特征函数, 或它对应的 L-函数有 Euler 积, 由于 $\mathcal{C}_{12}(\Gamma(1))$ 的维数是 1, 故它们都是十分自然的. 关于猜想 (III), 以后又由 Petersson 推广成 Ramanujan-Petersson 猜想, 1974 年被 Deligne 证明 (见正文中的定理 6). 关于 Ramanujan 函数还有许多有趣的算术性质, 在这里就不一一叙述了, 有兴趣的读者可参阅有关文献.

在本节的最后, 我们引入一个**模不变量函数** J :

$$J(z) = \frac{1728(2\pi)^{12}g_2(z)^3}{\Delta(z)}, \qquad z \in \mathfrak{H}.$$

它在函数论中扮演了十分重要的角色. 利用它我们可以在复平面和全模群的基本区域之间建立同构.

命题 1　由 $J(z)$ 决定的映射

$$J:\mathfrak{H}/\Gamma(1)\longrightarrow \mathbf{C},$$
$$z\longmapsto J(z)$$

是一一对应的.

此外，我们还有

命题 2　设 f 是 $\mathfrak{H}$ 上的亚纯函数，则下列诸性质彼此等价:

(1) f 是 $\Gamma(1)$ 的模函数 (即权为 0 的亚纯模形式);

(2) f 是两个权相同的 $\Gamma(1)$ 的模形式之商;

(3) f 是 J 的有理函数.

注　(1) 命题 1 表明 J 定义了 $\overline{\mathfrak{H}/\Gamma(1)}$ ($\mathfrak{H}/\Gamma(1)$ 的紧致化) 到 Riemann 球面 $S^2=\mathbf{C}\bigcup\{\infty\}$ 上的同构，而命题 2 则是一个熟知的事实，即扩充复平面 $\mathbf{C}$ 上的亚纯函数均为有理函数.

(2) $J(z)$ 的定义式中的系数的引进是为了使 J 在 ∞ 处的残数等于 1, 确切地说，即

$$J(z)=\frac{1}{q}+744+\sum_{n=1}^{\infty}c(n)q^n,\qquad z\in\mathfrak{H},\quad q=e^{2\pi iz}.$$

系数 $c(n)$ 也有许多有趣的算术性质，有兴趣的读者可参阅有关文献.

2. 同余子群上的模形式

设 Γ 为 $\Gamma(1)$ 的有限指数为 ν 的子群，命

$$\Gamma_\infty=\{T\in\Gamma:\ T:z\longrightarrow T(z)=z+b,\ b\ \text{为某个整数}\}.$$

则 Γ_∞ 为 Γ 的一个无限循环子群 (称为 Γ 的**平移子群**). 记其生成元为变换 $T_0:z\longrightarrow z+q$ (称为**极小变换**). 设 $\mathcal{R}=\Gamma_\infty\setminus\Gamma$ 是群 Γ 模 Γ_∞ 的右陪集代表元集. 对任意自然数 v, 称级数

$$\phi_v(z)=\sum_{T\in\mathcal{R}}\exp\left(\frac{2\pi i vT(z)}{q}\right)J_T(z)^{-k}$$

是群 Γ 的权为 $2k$, 特征为 v 的 **Poincaré 级数**, 其中

$$J_T(z) = (cz+d)^2, \qquad T = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbf{Z}).$$

类似于习题 20, 我们可以证明, 当 $v \geq 0$, $k \geq 1$ 时, Poincaré 级数 $\phi_v(z)$ 在 $\mathfrak{H}$ 的任一个紧子集上绝对且一致收敛; 进而 $\phi_v(z)$ 在 Γ 的每一个基域上绝对且一致收敛, 并且:

(1) $\phi_0(z)$ 在所有有限抛物顶点处是零, 而在 $\mathrm{i}\infty$ 处是 1;

(2) 若 $v \geq 1$, $\phi_v(z)$ 在所有抛物顶点处是零.

从而 $\phi_v(z)$ 是 Γ 的一个权为 $2k$ 的全纯模形式.

从上面也可看出, 当 $v \geq 1$ 时, Poincaré 级数 $\phi_v(z)$ 是尖点形式. 关于 Poincaré 级数我们有下面结果.

定理 3 设

$$f(z) = \sum_{n=1}^{\infty} a_n \exp\left(\frac{2\pi \mathrm{i} n z}{q}\right) \in \mathcal{C}_{2k}(\Gamma),$$

$\phi_v(z)$ 为群 Γ 的权为 $2k$, 特征为 v 的 Poincaré 级数, $v \geq 1$. 则我们有

$$(f, \phi_v) = \int_{\mathcal{D}} f(z)\overline{\phi_v(z)} y^{2(k-1)} \mathrm{d}x\mathrm{d}y$$

$$= q^{2k}(2k-2)!(4\pi)^{1-2k} v^{1-2k} a_v,$$

其中 $\mathcal{D}$ 为基域 $\mathfrak{H}/\Gamma$, 内积 (,) 是 Petersson 内积.

由此我们立即可以看出

定理 4 每一个 $f(z) \in \mathcal{C}_{2k}(\Gamma)$ 是 Poincaré 级数 $\phi_v(z) (v \geq 1)$ 的线性组合, 换句话说, 空间 $\mathcal{C}_{2k}(\Gamma)$ 可由 Poincaré 级数生成.

定理 3 的证明只需要基本的分析工具, 读者可参阅参考文献 [9]. 用类似的方法可以证明

命题 2 当 $v \geq 1$ 时, $(\phi_v, \phi_0) = 0$.

利用 Poincaré 级数在尖点处的性质可得

定理 5 模形式空间 $\mathcal{M}_{2k}(\Gamma)$ 中尖点形式子空间 $\mathcal{C}_{2k}(\Gamma)$ 关于 Petersson 内积的正交补子空间由 $\phi_{s,0}(z)$ 生成, 其中 s 过 Γ 的所有

不等价尖点. 这里 $\phi_{s,0}(z)$ 如下定义: 设 $S \in \Gamma(1)$ 使得 $S(s) = \mathrm{i}\infty$, 命 $\phi_0^*(z)$ 是群 $S\Gamma S^{-1}$ 的特征 $v = 0$ 的 Poincaré 级数, 它在 $\mathrm{i}\infty$ 的值为 1, 而在其余尖点处的值为 0. 定义 $\phi_{s,0}(z) = \phi_0^*(Sz)$.

定理中的这些 $\phi_{s,0}$ 我们均称为 **Eisenstein 级数**, 它们生成的这个空间称为 **Eisenstein空间**. 下面我们就 Γ 是主同余子群的情形来研究这些 Eisenstein 级数.

主同余子群 $\Gamma(N)$ 中的平移子群是由

$$\begin{pmatrix} 1 & rN \\ 0 & 1 \end{pmatrix}, \qquad r = 0, \pm 1, \pm 2, \cdots,$$

诱导的线性变换组成的, $\Gamma(N)$ 模其平移子群的陪集代表元可由 $\Gamma(N)$ 中对应于满足 $(c, d) = 1$ 和 $c \equiv 0,\ d \equiv 1 \pmod N$ 的数对 (c, d) 的变换

$$T = \begin{pmatrix} * & * \\ c & d \end{pmatrix}$$

充当 (当 $q = 1, 2$ 时, 可令 $d \geq 0$, 这是由于当且仅当 $N = 1, 2$ 时, $\pm I \in \Gamma(N)$). 于是 $\Gamma(N)$ 的权 $2k > 1$ 和特征 $v = 0$ 的 Poincaré 级数

$$\phi_0(z) = \sum_{\substack{(c,d) \equiv (0,1) (\bmod N) \\ \gcd(c,d)=1}} (cz + d)^{-2k}$$

是群 $\Gamma(N)$ 的权为 $2k$ 的 (全纯) 模形式. 它在 $\mathrm{i}\infty$ 处的值为 1, 而在所有其他的 (抛物) 尖点处的值是 0.

设 s 为一个有限抛物顶点, 而 $S \in \Gamma(1)$ 是使得 $S(s) = \mathrm{i}\infty$ 的变换, 则 $\phi_0(z)$ 的 S^{-1} 变换

$$\phi_0^*(z) = J_S(z)^k \phi_0(Sz)$$

是 $S^{-1}\Gamma(N)S = \Gamma(N)$ 的权为 $2k$ 的 (全纯) 模形式, 它在 s 处取值 1, 而在其他抛物顶点取值零.

设 $\Gamma(N)$ 模其平移子群的右陪集代表元集为 $\mathcal{R}$. $\phi_0^*(z)$ 的级数展开为:

$$\phi_0^*(z) = J_S(z)^k \phi_0(Sz) = J_S(z)^k \sum_{T\in\mathcal{R}} J_T(Sz)^k$$
$$= \sum_{T\in\mathcal{R}} (J_{TS}(z))^k = \sum_{T\in\mathcal{R}S} (J_T(z))^k.$$

设

$$S = \begin{pmatrix} x & y \\ p & q \end{pmatrix}, \quad xq - yp = 1,$$

则

$$S^{-1} = \begin{pmatrix} q & -y \\ -p & x \end{pmatrix}, \quad S^{-1}(\mathrm{i}\infty) = -\frac{q}{p}.$$

由于对应于每个满足 $\gcd(c,d)=1$ 和 $c \equiv p,\ d \equiv q \pmod N$ 的数对 (c,d), 只有一个 $\mathcal{R}S$ 中的变换以 (c,d) 为第二行, 于是我们有

$$\phi_0^*(z) = \sum_{\substack{(c,d)\equiv(p,q) \pmod N \\ \gcd(c,d)=1}} (cz+d)^{-2k}.$$

定义 $\Gamma(N)$ 的权 $2k(>1)$ 的**狭义 Eisenstein 级数**为级数

$$G_k^*(z;p,q;N) = \sum_{\substack{(c,d)\equiv(p,q) \pmod N \\ \gcd(c,d)=1}} (cz+d)^{-2k}.$$

由前面讨论可知 $G_k^*(z;p,q;N)$ 是群 $\Gamma(N)$ 的权为 k 的 (全纯) 模形式, 它在尖点 $-q/p$ 处的值为 1, 在其他尖点的值为 0. 易见当

$$(p,q) \equiv (p',q') \pmod N$$

或

$$(p,q) \equiv (-p',-q') \pmod N$$

时,

$$G_k^*(z;p,q;N) = G_k^*(z;p',q';N).$$

把上面的定义推广一些，我们定义 $\Gamma(N)$ 的权 $2k$ 的**广义 Eisenstein 级数**为级数

$$G_k(z;p,q;N)=\sum_{(c,d)\equiv(p,q)(\bmod N)}(cz+d)^{-2k}.$$

由上节定理 1 知，当 $k>1$ 时，上述级数在 $\mathfrak{H}$ 的任一紧子集上绝对且一致收敛. 从而当 $k>1$ 时，$G_k(z;p,q;N)$ 是 $\mathfrak{H}$ 上的一个全纯函数. 容易证明，如果 $\gcd(p,q,N)=r$, 则

$$G_k(z;p,q;N)=r^{-2k}G_k\left(z;\frac{p}{r},\frac{q}{r};\frac{N}{r}\right).$$

由此看出，以后我们总不妨假定 $\gcd(p,q,N)=1$.

当 $k>1$ 时，容易证明

$$G_k(z;p,q;N)$$
$$=\sum_{\substack{a=1\\ \gcd(c,d)=1}}^{q}\left(\sum_{\substack{n=1\\ na\equiv 1(\bmod N)}}^{\infty}n^{-2k}\right)G_k^*(z;ap,aq;N).$$

由此可知，$G_k(z;p,q;N)$ 是 $\Gamma(N)$ 的权为 $2k$ 的 (全纯) 模形式.

反之，同样有

$$G_k^*(z;p,q;N)$$
$$=\sum_{\substack{a=1\\ \gcd(a,q)=1}}^{q}\left(\sum_{\substack{n=1\\ na\equiv 1(\bmod N)}}^{\infty}\mu(n)n^{-2k}\right)G_k(z;ap,aq;N),$$

其中 μ 为 Möbius 函数. 因此广义 Eisenstein 级数与狭义 Eisenstein 级数生成的空间是一样的. 另一方面，从狭义 Eisenstein 级数在尖点处的性质及命题 2 可以看出，Eisenstein 空间是由这些级数生成的. 下面我们来研究它们的 Fourier 系数.

对余切函数的分式展开:

$$\pi\cot(z)=\lim_{m\to\infty}\sum_{n=-m}^{m}\frac{1}{z+n},$$

逐项微分可得

$$\frac{\mathrm{d}^{r-1}}{\mathrm{d}z^{r-1}}(\pi\cot(\pi z)) = (-1)^{r-1}(r-1)!\sum_{n=-\infty}^{\infty}\frac{1}{(z+n)^r}.$$

另一方面，当 $\operatorname{Im} z > 0$ 时我们有

$$\begin{aligned}\pi\cot(\pi z) &= -\mathrm{i}\pi\frac{1+\mathrm{e}^{2\pi\mathrm{i}z}}{1-\mathrm{e}^{2\pi\mathrm{i}z}}\\ &= -\mathrm{i}\pi(1+\mathrm{e}^{2\pi\mathrm{i}z})\left(\sum_{n=0}^{\infty}\mathrm{e}^{2\pi\mathrm{i}nz}\right)\\ &= (-\pi\mathrm{i})\left(1+2\sum_{n=1}^{\infty}\mathrm{e}^{2\pi\mathrm{i}nz}\right).\end{aligned}$$

从而推出

$$\sum_{n=-\infty}^{\infty}\frac{1}{(z+n)^r} = \frac{(-2\pi\mathrm{i})^r}{(r-1)!}\sum_{n=1}^{\infty}n^{r-1}\mathrm{e}^{2\pi\mathrm{i}nz},$$

$$r > 1,\ \operatorname{Im} z > 0.$$

由此我们可得

定理 6 命

$$A = \begin{cases} 0, & 若\ p \not\equiv 0 \pmod N, \\ \displaystyle\sum_{\substack{n\equiv q \pmod N \\ n\neq 0}} n^{-2k}, & 若\ p \equiv 0 \pmod N, \end{cases}$$

$$\sigma_m(n;p,q) = \sum_{\substack{d\mid n \\ n/d\equiv p \pmod N}} d^m \mathrm{e}^{2\pi\mathrm{i}dq/N}.$$

则当 $k > 1$ 时，有

$$G_k(z;p,q;N) = A + \frac{(-1)^k(2\pi)^{2k}}{N^{2k}(2k-1)!}\sum_{n=1}^{\infty}[\sigma_{2k-1}(n;p,q) + \sigma_{2k-1}(n;-p,-q)]\mathrm{e}^{2\pi\mathrm{i}nz/N}.$$

作为定理的一个推论，我们有：当 $k>1$ 时，

$$G_k(z)=2\zeta(2k)+\frac{2(-1)^k(2\pi)^k}{(2k-1)!}\sum_{n=1}^{\infty}\sigma_{2k-1}(n)\mathrm{e}^{2\pi\mathrm{i}nz},$$

其中 $\zeta(s)$ 为 Riemann zeta 函数，$\sigma_m(n)=\sum\limits_{d|n}d^m$ 是除数函数.

3. Theta 级数

前两节我们借助 Poincaré 级数和 Eisenstein 级数给出了模形式的具体例子. 在这一节中，我们将介绍一个新的构造方法，即利用 Theta 级数构造模形式.

首先我们来考虑一个算术问题：设 $A=(a_{ij})$ 是一个 r 阶正定对称方阵，且 A 为整的，即 $2|a_{ii}$ 且 $a_{ij}(i\neq j)$ 是整数. 这样当

$${}^{\mathrm{t}}x=(x_1,\cdots,x_r)$$

(这里 ${}^{\mathrm{t}}x$ 表示矩阵 x 的转置) 为整向量时，

$$Q(x)=\frac{1}{2}\,{}^{\mathrm{t}}xAx=\frac{1}{2}\sum_{i,j=1}^{r}a_{ij}x_ix_j$$

是整数. 这样的二次型 $Q(x)$ 是一个整的正定二次型. 给出一个整数 n, 我们记 Diophantine 方程 $n=Q(x)$ 的整数解的个数为 $r_Q(n)$. 求 $r_Q(n)$ 是数论的一个经典问题. 结合二次型 Q 定义

$$\theta(z,Q)=\sum_{M}\mathrm{e}^{2\pi\mathrm{i}Q(M)z}\quad(\mathrm{Im}\,z>0),$$

这里 $M={}^{\mathrm{t}}(m_1,\cdots,m_r)$ 跑遍所有的整向量，我们称之为二次型 Q 所决定的 **theta 级数**. 显然

$$\theta(z,Q)=\sum_{n=0}^{\infty}r_Q(n)\mathrm{e}^{2\pi\mathrm{i}nz}.$$

于是求 $r_Q(n)$ 的问题就转化求 theta 函数 $\theta(z,Q)$ 的 Fourier 系数.

由于矩阵 A 是正定的，故 A 的最小特征值 $c>0$. 从而我们有 ${}^{\mathrm{t}}xAx \geq c\ {}^{\mathrm{t}}xx$, 于是

$$|\theta(z,Q)| \leq \left(\sum_{n=-\infty}^{+\infty} \mathrm{e}^{-2\pi cyn^2}\right)^r, \qquad y=\operatorname{Im} z>0.$$

从而它在上半平面 $\mathfrak{H}$ 是解析的. 此外，显然有

$$\theta(z+1,Q)=\theta(z,Q).$$

为了让问题限制在整权模形式的范围里, 今后我们约定 $r=2k$ 是一个偶数.

矩阵 A 的行列式 D 称为**二次型 Q 的行列式**,

$$\Delta=(-1)^k D$$

称为 Q 的**判别式**. 由于 A 是整对称的正定矩阵，所以它的伴随矩阵 DA^{-1} 也是一个整对称的正定矩阵. 于是我们可以找到一个最小的正整数 N, 使得 $NA^{-1}=A^*$ 是一个整矩阵，数 N 称为二次型 Q 的**级**(level). 对应的二次型

$$Q^*(x)=\frac{1}{2}\ {}^{\mathrm{t}}xNA^{-1}x$$

称为 Q 的**伴随二次型**. 显然 $N|D$, 并且 Q^* 是本原的，即不存在任意整数 $v>1$, 使得 $-Q^*/v$ 是一个整形式. 换句话说，$\dfrac{1}{2}a_{ii}^*$ 和 a_{ij}^* 的最大公因子是 1. Q^* 的伴随二次型 Q^{**} 对应的矩阵

$$A^{**}=N^*A^{*-1}=\frac{N^*}{N}A=\frac{1}{\beta}A,$$

其中 $\beta=\gcd\left(\dfrac{1}{2}a_{ii},a_{ij}\right)$. 特别地，若 Q 是本原的，则 $N=N^*$, 即 Q 与其伴随二次型 Q^* 有相同的级，并且 $Q^{**}=Q$. 一般而言,

$$N^*|N, \quad D^*=N^{2k}D^{-1},$$

于是 $D|N^{2k}$. 总结上面的讨论，我们有如下结果:

命题 3　二次型 Q 的行列式 D 和级 N 满足关系 $N \mid D \mid N^{2k}$, 因此 N 和 D 有相同的素因子. 进而当级 N 一定时, 在所有 $2k$ 个变数的二次型中, 对应的判别式 Δ 的值只有有限多种可能.

本节的基本结果是 $\theta(z,Q) \in \mathcal{M}(N,k,\varepsilon)$, 其中

$$\varepsilon(n) = \begin{cases} \left(\dfrac{\Delta}{n}\right), & 若\, n > 0, \\ (-1)^k \varepsilon(-n), & 若\, n < 0, \end{cases}$$

式中 $\left(\frac{}{-}\right)$ 是 Jacobi 符号.

对 ${}^t x \in Z^r$, 令

$$\theta(z,x,Q) = \sum_M \exp(2\pi i z Q(M+x)).$$

利用 Poisson 求和公式可得

定理 7 (Jacobi 反转公式)

$$\theta(z,x,Q) = \frac{1}{\sqrt{(-iz)^r \det A}} \sum_M \exp\left(\frac{\pi i}{z} A^{-1}[M] + 2\pi i\ {}^t x M\right).$$

特别地我们有

$$\theta(z,Q) = \frac{1}{\sqrt{(-iz)^r \det A}} \theta\left(-\frac{1}{Nz}, Q^*\right).$$

由此出发, 我们可以证明 $\theta(z,Q)$ 是一个模形式. 这样求 $r_Q(n)$ 的问题就化为讨论模形式 $\theta(z,Q)$ 的 Fourier 系数. 这同时也给了我们一种构造模形式的方法.

现在把上面这种利用二次型构造 theta 级数的方法一般化, 我们用球函数来重新定义 theta 级数. 设 A 是一个 r 阶正定实对称矩阵. 利用线性变换 $y = Bx$, 我们可以把二次型 ${}^t x A x$ 对角化

$$\sum_{i=1}^r y_i^2 = {}^t x A x = {}^t y\ {}^t(B^{-1}) A B^{-1} y,$$

即: $I = {}^t(B^{-1}) A B^{-1}$, 或 $A = {}^t B B$ (B 是一个实矩阵).

定义关于二次型 $Q={}^{\mathrm{t}}xAx$ 的球函数是一个 r 元函数 $f(x)$, 它满足方程

$$\sum_{i=1}^{r}\frac{\partial^2 f}{\partial y_i^2}=0,$$

换句话说, 它满足方程

$$\sum_{i,j,k}\frac{\partial^2 f}{\partial x_j\partial x_k}\frac{\partial x_j}{\partial y_i}\frac{\partial x_k}{\partial y_i}=0.$$

令 $A^{-1}=(a_{ij}^*)$, 则 $A^{-1}=B^{-1}\,{}^{\mathrm{t}}B^{-1}$. 于是 $f(x)$ 是关于二次型 Q 的球函数的充分必要条件是

$$\sum_{i,j,k}a_{ij}^*\frac{\partial^2 f}{\partial x_j\partial x_k}=0.$$

我们对 r 元实函数定义一个内积

$$(f,g)_A=\int_{{}^{\mathrm{t}}xAx\leq 1}f(x)\overline{g(x)}\mathrm{d}x_1\cdots\mathrm{d}\,x_r\quad x=(x_1,\cdots,x_r)\in\mathbf{R}^r. \tag{a.4}$$

关于球函数我们有下面结论:

定理 8 设 $f(x)$ 是一个复系数的 r 元 v 阶齐次多项式. 下面三个条件等价:

(1) $f(x)$ 是一个关于 ${}^{\mathrm{t}}xAx$ 的球函数;

(2) $f(x)$ 同任何次数小于 v 的齐次多项式的内积为 0;

(3) $f(x)$ 是一些 $({}^{\mathrm{t}}\xi Ax)^v$ 形式的函数的线性组合, 其中 $\xi\in\mathbf{C}^r$ 且 ${}^{\mathrm{t}}\xi A\xi=0$.

现在我们可以把定理 7 推广至下式:

$$\theta(z;Q,P)=\sum_{M}P(M)\mathrm{e}^{2\pi\mathrm{i}Q(M)z},$$

其中 $P(x)$ 是关于二次型 $Q(x)$ 的 v 阶球函数. 以后我们总假定 Q 是一个 $2k$ 个变量的整的正定的二次型. $P(x)$ 是关于二次型 $Q(x)$ 的 v 阶球函数.

定理 9(Schoeneberg)　设 $P(x)$ 是关于 $Q(x)$ 的 v 阶球函数, $P^*(x)=P(A^{-1}x)$ 是它的伴随函数 (二次型 $Q^*(x)$ 的球函数). 则

$$\sum_M P(M+x)\exp(2\pi\mathrm{i}Q(M+x)z)$$
$$=\frac{\mathrm{i}^k}{\sqrt{D}z^{k+v}}\sum_M P^*(M)\exp\left(-\frac{\pi\mathrm{i}}{z}\,{}^{\mathrm{t}}MA^{-1}M+2\pi\mathrm{i}\,{}^{\mathrm{t}}Mx\right).$$

令 $H_N=\begin{pmatrix}0&-1\\N&0\end{pmatrix}$, $\theta(z;Q,P)=\sum\limits_M P(M)\exp(2\pi\mathrm{i}Q(M))$.

推论 3　我们有

$$\theta(z;Q,P)=\frac{\mathrm{i}^kN^{(k+v)/2}}{\sqrt{D}}\theta(z;Q^*,P^*)|_{k+v}H_N.$$

推论 4　对一个满足 $Ah\equiv 0(\bmod N)$ 的整向量 h, 定义

$$\theta(z;Q,P,h)=N^{-v}\sum_{n\equiv h(\bmod N)}P(n)\exp\left(\frac{2\pi\mathrm{i}Q(n)z}{N^2}\right).$$

则

$$\theta(z;Q,P,h)$$
$$=\frac{\mathrm{i}^k}{\sqrt{D}}\sum_{\substack{g(\bmod N)\\Ag\equiv 0(\bmod N)}}\exp\left(\frac{2\pi\mathrm{i}\,{}^{\mathrm{t}}gAh}{N^2}\right)\theta(z;Q,P,g)|_{k+v}H_1.$$

很容易验证

$$\theta(z+1;Q,P,h)=\exp\left(\frac{2\pi\mathrm{i}Q(h)}{N^2}\right)\theta(z;Q,P,h).$$

结合上面的讨论可以看出由 theta 函数 $\theta(z;Q,P,h)$ 生成的向量空间在全模群的作用下是不变的. 此外, 这些级数显然在 ∞ 处全纯, 并且当 $v>0$ 时, 它们在 ∞ 处的值为 0. 下面这个定理告诉我们这些 theta 函数在 $\Gamma(N)$ 作用下不变. 于是我们就可以断言这些 theta 级数是级为 N 的模形式 (当 $v\geq 1$ 时, 它们是尖点形式).

定理 10(Schoenberg) 我们有

$$\theta(z;Q,P,h)|_{k+v}\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \exp\left(\frac{2\pi\mathrm{i}abQ(h)}{h^2}\right)\varepsilon(d)\theta(z;Q,P,ah),$$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N),$$

其中 ε 是一个模为 N 的实特征标，且满足 $\varepsilon(-1)=(-1)^k$. 特别地，当 $\gamma\in\Gamma(N)$ 时，

$$\theta(z;Q,P,h)|_{k+v}\gamma = \theta(z;Q,P,h).$$

让我们回到本节开始的问题上，为简单起见，我们只就 $N=1$ 的情况来讨论. 此时

$$\theta(z+1,Q)=\theta(z,Q), \quad \theta(z,Q)=\left(\frac{z}{\mathrm{i}}\right)^k\theta\left(\frac{-1}{z};Q\right).$$

现在我们还假定 $4|k$, 于是 $\theta(z;Q)$ 是一个关于全模群的权为 k 的模形式，此时利用第一节讨论的全模群上模形式空间的结构可得

$$\theta(z;Q)=\frac{1}{\zeta(2k)}G_k(z)+g(z),$$

其中 $g(z)$ 是一个尖点形式. 于是利用 Eisenstein 级数的 Fourier 系数及 Ramanujan-Petersson 猜想可以推出

$$r_Q(n)=\frac{(2\pi)^k}{\Gamma(k)\zeta(k)}\sigma_{k-1}(n)+O(n^{k/2}).$$

从而我们就得到了一个 $r_Q(n)$ 的渐近公式. 特别地，当 $k=4$ 时，由于 $\dim\mathcal{M}(\Gamma(1),4)=1$, 所以

$$\theta(z;Q)=\frac{1}{a\zeta(8)}G_4(z)=1+240\sum_{n=1}^{\infty}\sigma_3(n)\exp(2\pi\mathrm{i}nz).$$

于是当 $n\geq 1$ 时， $r_Q(n)=240\sigma_3(n)$. 这样的二次型的一个例子是

$$Q(x)=\frac{1}{2}\sum_{i=1}^{8}x_i^2+\frac{1}{2}\left(\sum_{i=1}^{8}x_i\right)^2-x_1x_2-x_2x_8.$$

对一般的级为 N 的 r 元二次型，我们可以类似地讨论. theta 级数理论是数学的一个重要分支，有关它的系统介绍可以参见参考文献 [37] 和 [38]. 对 Schoenberg 结果的更多的讨论可以参见参考文献 [39] 和 [18]. 至于二次型的表示问题的历史背景可参见参考文献 [36], 它的更一般的形式的研究可参见参考文献 [1].

附加参考文献

[36] E. Grosswald, *Representein of Integers as Sums of Squares*, Springer-Verlag, New York, 1985.

[37] J.-I. Igusa, *Theta Functions*, Springer-Verlag, New York, 1974.

[38] D. Mumford, *Tata Lectures on Theta*, I, II, III, Birkhauser, Boston, 1983.

[39] B. Schoenberg, *Elliptic Modular Functions*, Springer-Verlag, New York, 1974.

第八章　自守形式和自守表示

在这一章，我们将介绍阿代尔群上的自守形式和自守表示理论的基础知识，这些是经典模形式理论的推广.

§1　自守形式

在第七章，我们研究了定义在 Poincaré 上半平面 $\mathfrak{H}$ 上的模形式理论. 在这一节里，我们将把这些模形式作为 $\mathrm{GL}_2(A_{\mathbf{Q}})$ 上的自守形式来重新描述，进而把模形式的概念推广为整体域上的自守形式.

在这一章中，我们将用到 Lie 群，Lie 代数及其表示论的一些知识，不熟悉这方面内容的读者可以参阅有关书籍，例如参考文献 [18], [31], [35] 和 [38].

设 $\mathrm{GL}_2^0(\mathbf{R})$ 是 $\mathrm{GL}_2(\mathbf{R})$ 中具有正行列式值的 2×2 实矩阵全体构成的群，同 $\mathrm{SL}_2(\mathbf{Z})$ 类似，它能以线性变换的方式作用在 $\mathfrak{H}$ 上，赋予 $\mathrm{GL}_2(\mathbf{R})$ 以通常的 Lie 群结构，则 $\mathrm{GL}_2^0(\mathbf{R})$ 是它的一个连通分支. 我们又用 $\mathcal{Z}$ 表示 GL_2 的中心，于是

$$\mathcal{Z}(\mathbf{R}) = \left\{ \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \in \mathrm{GL}_2(\mathbf{R}) \right\} \cong \mathbf{R}^{\times}.$$

今后，在不致引起混乱时，我们将把 $\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$ 简记为 a.

习题 1　(1) 证明 $\mathrm{GL}_2^0(\mathbf{R})$ 在 $\mathfrak{H}$ 上的作用是可迁的，即对 $\mathfrak{H}$ 上任意两个元 z_1 和 z_2，存在 $\gamma\in \mathrm{GL}_2^0(\mathbf{R})$，使得 $z_1=\gamma z_2$.

(2) 证明 i 在 $\mathrm{GL}_2^0(\mathbf{R})$ 中的稳定子群，即将 i 映为 i 的线性变换群，是 $\mathcal{Z}(\mathbf{R})\mathrm{SO}_2(\mathbf{R})$.

对 $\mathrm{GL}_2(\mathbf{R})$ 中任意元素 g_∞, 存在 $x, y, z \in \mathbf{R}$, $y, z > 0$, 以及

$$r(\theta) = \begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix} \in \mathrm{SO}_2(\mathbf{R}),$$

使得 g_∞ 可唯一地写为

$$g_\infty = z\begin{pmatrix} y & x \\ 0 & 1 \end{pmatrix} r(\theta).$$

这样，将 g_∞ 映为 $g(\mathrm{i}) = x + \mathrm{i}y$ 的映射导出了同化 (identification):

$$\mathrm{GL}_2^0(\mathbf{R})/\mathcal{Z}(\mathbf{R})\mathrm{SO}_2(\mathbf{R}) \approx \mathfrak{H}.$$

任给一个 $\mathrm{GL}_2^0(\mathbf{R})$ 上的函数

$$\begin{aligned} \phi(g_\infty) &= \phi\left(z\begin{pmatrix} y & x \\ 0 & 1 \end{pmatrix} r(\theta)\right) \\ &= \phi\left(\begin{pmatrix} y & x \\ 0 & 1 \end{pmatrix}\right)\mathrm{e}^{\mathrm{i}k\theta}, \quad g_\infty \in \mathrm{GL}_2(\mathbf{R}), \end{aligned}$$

它定义出 $\mathfrak{H}$ 上的一个函数 f

$$f(x + \mathrm{i}y) = y^{-k/2}\phi\left(\begin{pmatrix} y & x \\ 0 & 1 \end{pmatrix}\right).$$

习题 2　证明 ϕ 在 $\mathrm{SL}_2(\mathbf{Z})$ 左作用下不变的充分必要条件是:

$$f(\tau) = f|_k\gamma(\tau) = (c\tau + d)^{-k} f(\gamma\tau),$$

$$\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbf{Z}), \quad \tau \in \mathfrak{H}.$$

这样，我们看到一个全模群上权 k 的模形式 f 可以化为一个 $\mathrm{GL}_2(\mathbf{R})$ 上的函数 ϕ, 它满足条件：对任意的 $\gamma \in \mathrm{SL}_2(\mathbf{Z})$, $z > 0$, $r(\theta) \in \mathrm{SO}_2(\mathbf{R})$ 和 $g_\infty \in \mathrm{GL}_2^0(\mathbf{R})$, 有

$$\phi(\gamma g_\infty r(\theta) z) = \phi(g_\infty)\mathrm{e}^{\mathrm{i}k\theta}, \tag{1.1}$$

当然，ϕ 还应该具有其他一些好的性质.

对 $\mathbf{Q}$ 的每个有限位 p, 以 $\mathbf{Z}_p$ 表示 p-adic 数域 $\mathbf{Q}_p$ 的整数环. 于是 $\mathrm{GL}_2(\mathbf{Z}_p)$ 是 $\mathrm{GL}_2(\mathbf{Q}_p)$ 的紧开子群. 定义阿代尔群 $\mathrm{GL}_2(A_{\mathbf{Q}})$

是 $\{\mathrm{GL}_2(\mathbf{Q}_p)\}$ 关于 $\{\mathrm{GL}_2(\mathbf{Z}_p)\}$ 的限制直积. 显然 $\mathrm{GL}_2(\mathbf{Q})$ 可以对角地嵌入到 $\mathrm{GL}_2(A_{\mathbf{Q}})$ 中. 以后为方便起见, 我们仍用 $\mathrm{GL}_2(\mathbf{Q})$ 来表示其嵌入后的像. 令

$$\Omega = \mathrm{GL}_2^0(\mathbf{R}) \prod_p \mathrm{GL}_2(\mathbf{Z}_p),$$

它是 $\mathrm{GL}_2(A_{\mathbf{Q}})$ 的一个开子群. 利用 SL_2 的强逼近定理可得

$$\mathrm{GL}_2(A_{\mathbf{Q}}) = \mathrm{GL}_2(\mathbf{Q})\Omega.$$

容易验证,

$$\mathrm{GL}_2(\mathbf{Q}) \bigcap \Omega = \mathrm{SL}_2(\mathbf{Z}).$$

于是, 一个满足 (1.1) 式的 $\mathrm{GL}_2^0(\mathbf{R})$ 上的函数 ϕ 可以扩张为 $\mathrm{GL}_2(A_{\mathbf{Q}})$ 上的函数 F, 它在 $\prod\limits_p \mathrm{GL}_2(\mathbf{Z}_p)$ 的右作用下不变, 在 $\mathrm{GL}_2(\mathbf{Q})$ 的左作用下也不变. 即, 对任意的 $\gamma \in \mathrm{GL}_2(\mathbf{Q})$, $g \in \mathrm{GL}_2(A_{\mathbf{Q}})$, $z > 0$, $\gamma(\theta) \in \mathrm{SO}_2(\mathbf{R})$ 和 $\beta \in \prod\limits_p \mathrm{GL}_2(\mathbf{Z}_p)$, 有

$$F(\gamma g r(\theta)\beta) = F(g)\mathrm{e}^{\mathrm{i}k\theta}. \tag{1.2}$$

又由于 $\mathrm{GL}_2(A_{\mathbf{Q}})$ 的中心为

$$\begin{aligned} \mathcal{Z}(A_{\mathbf{Q}}) &= \left\{ \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \in \mathrm{GL}_2(A_{\mathbf{Q}}) \right\} \\ &\cong I_{\mathbf{Q}} = \mathbf{Q}^{\times}\mathbf{R}_{>0} \prod_p \mathcal{U}_p, \end{aligned}$$

其中 $\mathbf{R}_{>0}$ 是正实数集, 所以公式 (1.2) 对所有的 $z \in I_{\mathbf{Q}}$ 也成立.

我们用 $\mathrm{GL}_2(A_{\mathbf{Q}}^f)$ 表示 $\mathrm{GL}_2(A_{\mathbf{Q}})$ 的一个子群, 它是由那些在 Archimedes 位处平凡的元素组成的. 故

$$\mathcal{K}^f = \prod_p \mathrm{GL}_2(\mathbf{Z}_p)$$

是它的标准最大紧子群. 对任意自然数 N, $\mathcal{K}^f$ 包含有同余子群

$$\mathcal{K}_0^f(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathcal{K}^f : \text{对 } \mathbf{Q} \text{ 的有限位 } p, \right.$$

$$\left. \mathrm{ord}_p c \geq \mathrm{ord}_p N \right\}.$$

习题 3　证明同余子群 $\mathcal{K}_0^f(N)$ 关于 $\mathcal{K}^f$ 的阶是有限的, 且

$$\mathrm{GL}_2(\mathbf{Q}) \bigcap \mathrm{GL}_2^0(\mathbf{R}) \mathcal{K}_0^f(N) = \Gamma_0(N).$$

我们已经知道, 一个 Dirichlet 特征标 χ 可以提升为 $I_{\mathbf{Q}}/\mathbf{Q}^\times$ 的伊代尔类特征标, 为方便起见, 两者均以 χ 来表示. 这样, 一个权 k, 水平 N, 特征标为 χ 的模形式 f 可以化为一个满足关系

$$F(\gamma g r(\theta) z \beta) = \chi(z)\chi(d)F(g)\exp(\mathrm{i}k\theta),$$

且有好的解析性质的 $\mathrm{GL}_2(A_{\mathbf{Q}})$ 上的函数 F, 其中 $\gamma \in \mathrm{GL}_2(\mathbf{Q})$, $g \in \mathrm{GL}_2(A_{\mathbf{Q}})$, $z \in \mathcal{Z}(A_{\mathbf{Q}})$, $r(\theta) \in \mathrm{SO}_2(\mathbf{R})$, 以及

$$\beta = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathcal{K}_0^f(N).$$

这就导出了下述关于阿代尔群 $\mathrm{GL}_2(A_{\mathbf{Q}})$ 上自守形式的概念:

设 η 是伊代尔群 $I_{\mathbf{Q}}/\mathbf{Q}^\times$ 的伊代尔类特征标, F 是 $\mathrm{GL}_2(A_{\mathbf{Q}})$ 上的复值函数, 如果 F 满足:

(1) 对任意的 $\gamma \in \mathrm{GL}_2(\mathbf{Q})$, $g \in \mathrm{GL}_2(A_{\mathbf{Q}})$ 和 $z \in \mathcal{Z}(A_{\mathbf{Q}}) = I_{\mathbf{Q}}$ 有

$$F(\gamma g z) = \eta(z)F(g).$$

(2) F 是右 $\mathcal{K}(= O_2(\mathbf{R})\mathcal{K}^f)$ 有限的, 即由 F 被 $\mathcal{K}$ 中元素做右变换后所得函数生成的空间是有限维的;

(注　该条件指出, 对几乎所有的 p, F 关于 $\mathrm{GL}_2(\mathbf{Z}_p)$ 的右作用是不变的. 从而存在正整数 N, 使得

$$\mathcal{K}^f(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathcal{K}^f : \text{对 } \mathbf{Q} \text{ 的有限位 } p, \right.$$

$$\left.\begin{array}{l}\mathrm{ord}_p(a-1)\geq \mathrm{ord}_p N, \mathrm{ord}_p b\geq \mathrm{ord}_p N\,,\\ \mathrm{ord}_p c\geq \mathrm{ord}_p N, \mathrm{ord}_p(d-1)\geq \mathrm{ord}_p N\end{array}\right\}$$

在 F 上的右作用是平凡的. 此外, $\mathrm{O}_2(\mathbf{R})$ 对 F 的右变换产生了一个 $\mathrm{O}_2(\mathbf{R})$ 的有限维表示.)

(3) F 满足一些解析条件.

那么我们称 F 是 $\mathrm{GL}_2(A_{\mathbf{Q}})$ 上特征标为 η 的**自守形式**.

现在我们来解释一下 (3) 中的解析条件是什么. 首先我们知道经典的模形式是 $\mathfrak{H}$ 上的整函数, 那么这一条件对 $\mathrm{GL}_2(A_{\mathbf{Q}})$ 上的函数如何体现呢? 我们将借助于微分算子. Lie 群, Lie 代数的基本知识告诉我们:

$$X=\begin{pmatrix}0&1\\0&0\end{pmatrix},\quad Y=\begin{pmatrix}0&0\\1&0\end{pmatrix},$$

$$U=\begin{pmatrix}1&0\\0&-1\end{pmatrix},\quad Z=\begin{pmatrix}1&0\\0&1\end{pmatrix}$$

生成了 $\mathrm{GL}_2(\mathbf{R})$ 的 Lie 代数 $\mathfrak{gl}_2(\mathbf{R})$, 并且, X,Y,Z 生成了 $\mathrm{SL}_2(\mathbf{R})$ 的 Lie 代数 $\mathfrak{sl}_2(\mathbf{R})$; X 和 U 生成了 $\mathrm{SL}_2(\mathbf{R})$ 的 Borel 子群

$$B=\left\{\begin{pmatrix}x&y\\0&z\end{pmatrix}\in \mathrm{SL}_2(\mathbf{R})\right\}$$

的 Lie 代数; $X-Y$ 生成了 $\mathrm{SO}_2(\mathbf{R})$ 的 Lie 代数; Z 生成了中心 $\mathcal{Z}(\mathbf{R})$ 的 Lie 代数. 对 $\mathfrak{gl}_2(\mathbf{R})$ 中的任意元 W, 我们可以定义 $\mathrm{GL}_2(\mathbf{R})$ 上函数空间的左不变微分算子, 为简单起见, 我们仍以原来的符号表示

$$(Wf)(g)=\frac{\mathrm{d}}{\mathrm{d}t}f(g\mathrm{e}^{tW})|_{t=0},\quad g\in \mathrm{GL}_2(\mathbf{R})\,,$$

其中 f 是 $\mathrm{GL}_2(\mathbf{R})$ 上的函数. 在这些微分算子中, 那些在左变换和右变换下都不变的微分算子是由 $\mathfrak{gl}_2(\mathbf{R})$ 的通用包络代数 (universal enveloping algebra) 的中心里的元素诱导出的. 这个中心在 $\mathrm{SL}_2(\mathbf{R})$ 的情形是由 Casimir 算子

$$D=\frac{1}{2}U^2+XY+YX$$

生成；在 $\mathrm{GL}_2(\mathbf{R})$ 的情况该中心则由 D 和 Z 生成.

设 ϕ 是 $\mathrm{GL}_2(\mathbf{R})$ 上满足

$$\phi(gzr(\theta)) = \phi(g)\mathrm{e}^{\mathrm{i}k\theta}, \quad g \in \mathrm{GL}_2(\mathbf{R}),\ z > 0,\ r(\theta) \in \mathrm{SO}_2(\mathbf{R})$$

的一个函数. 容易验证

$$(X - Y)\phi = \mathrm{i}k\phi.$$

又因为

$$U = XY - YX,$$

所以

$$(XY + YX)\phi = (2XY - U)\phi = 2X(X - \mathrm{i}k)\phi - U(\phi).$$

命

$$f(x + \mathrm{i}y) = \phi\left(y^{1/2}\begin{pmatrix} y & x \\ 0 & 1 \end{pmatrix}\right).$$

由于 X 和 U 在 Borel 子群 B 的 Lie 代数中，从而有

$$X\phi = y\frac{\partial f}{\partial x}, \quad U\phi = 2y\frac{\partial f}{\partial y}.$$

于是，$D\phi$ 对应了

$$2y^2\left(\frac{\partial^2}{\partial x^2} + \frac{\partial^2}{\partial y^2} - \frac{\mathrm{i}k}{y}\frac{\partial}{\partial x}\right)(f) = \Delta f.$$

算子 Δ 是一个椭圆算子，它是 Laplace-Beltrami 算子的推广. 当 $k = 0$ 时，它就是通常所述的 Laplace 算子. 由于整函数是 Laplace 算子的特征值为 0 的特征函数，于是我们自然地把“模形式是 $\mathfrak{H}$ 上的整函数”这一条件转化为“自守形式均为 Casimir 算子的特征函数或者是这些特征函数的线性组合”. 注意到，Maass 形式是 Laplace 算子的有非 0 特征值的特征函数，所以这里自守形式的定义同时包含了在 $\mathfrak{H}$ 上全纯的模形式和在 $\mathfrak{H}$ 上实解析的 Maass 形式.

经典模形式的另一个解析性质是在尖点处全纯. 在第七章我们已经看到, 这个条件可以用函数的增长条件来表达. 在这里, 对一个 $\mathrm{GL}_2(A_{\mathbf{Q}})$ 上的自守形式 F, 我们要求存在非负常数 δ, 使得当 $y\in\mathbf{R}$ 且 $y\longrightarrow\infty$ 时, F 满足

$$\left|F\left(\begin{pmatrix} y & 0 \\ 0 & 1 \end{pmatrix} g\right)\right| = O(y^{\delta}), \quad g\in\mathrm{GL}_2(\mathbf{R})\mathcal{K}^f, \tag{1.3}$$

并且在 $\mathrm{GL}_2(\mathbf{R})\mathcal{K}^f$ 的任意紧子集上, 上述的增长界是一致的. 需要再说明一下的是: 当

$$g=\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

时, 这一条件刻画了函数 F 在尖点 $\mathrm{i}\infty$ 处的性质; 而随着 g 在 $\mathcal{K}^f$ 中的变化, 我们可以得到 F 在其他尖点处的性质.

习题 4 设 f 是一个经典模形式. 由前面的讨论可知, f 对应了一个 $\mathrm{GL}_2(A_{\mathbf{Q}})$ 上的函数 F. 证明 F 满足增长条件 (1.3) 与 f 在尖点处全纯是一致的.

类似地, 对整体域 K, 设 η 是 $I_K/K^{\times}$ 的拟特征标. 定义 $\mathrm{GL}_2(A_K)$ 上特征标为 η 的**自守形式** F 是 $\mathrm{GL}_2(A_K)$ 的一个复值函数, 并且 F 满足:

(1′) 对任意的 $\gamma\in\mathrm{GL}_2(K)$, $g\in\mathrm{GL}_2(A_K)$ 和 $z\in I_K=\mathcal{Z}(A_K)$, 有 $F(\gamma gz)=\eta(z)F(g)$;

(2′) 设 $\mathcal{K}$ 是 $\mathrm{GL}_2(K_v)$ 的标准最大紧子群的乘积, 其中 v 过 K 的位集, 则 F 是右 $\mathcal{K}$ 有限的;

(3′) F 满足一定的解析条件.

同前面一样, 这些解析条件包括有增长条件, 并且当 K 是数域时, 在每个 Archimedes 位 v 处, 通过将 $g\in\mathrm{GL}_2(A_K)$ 中除 v 外的其余分支固定, 由 $F(g)$ 可得 $\mathrm{GL}_2(K_v)$ 上的函数. 我们要求这个函数位于一个由 Casimir 算子的特征函数生成的有限维向量空间中. 当 v 是实位时, Casimir 算子 D 同前面所述的一样; 而当 v

是复位时，则存在两个 Casimir 算子 D' 和 D''，它们位于 $\mathrm{GL}_2(\mathbf{C})$ 的 Lie 代数的通用包络代数之中心里.

设 F 是 $\mathrm{GL}_2(A_K)$ 上的自守形式. 由于 F 在 $\mathrm{GL}_2(K)$ 的左作用下不变，所以对任意的 $g \in \mathrm{GL}_2(A_K)$,

$$F\left(\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} g\right)$$

是 $K\backslash A_K$ 上的连续函数. 因此，像经典模形式一样我们可以给出 F 的 "Fourier 展开". 给定 A_K/K 的一个非平凡加法特征 ψ，我们已经知道 A_K/K 的所有非平凡加法特征均可写成 ψ^t $(t \in K^\times)$ 的形式. 对 $\alpha \in K$，命

$$W_\alpha(g) = \int_{K\backslash A_K} F\left(\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} g\right) \psi^{-\alpha}(x)\mathrm{d}x,$$

其中 $\mathrm{d}x$ 是 A_K 上使得 A_K/K 的体积为 1 的 Haar 测度. 则我们有下面形式的 Fourier 展开

$$F\left(\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} g\right) = \sum_{\alpha \in K} W_\alpha(g)\psi(\alpha x), \quad x \in A_K.$$

从 W_α 的定义以及 F 在

$$\left\{\begin{pmatrix} \beta & 0 \\ 0 & 1 \end{pmatrix} : \beta \in K^\times\right\}$$

左作用下不变可知：对 $\alpha \in K^\times$ 有

$$W_\alpha(g) = W_1\left(\begin{pmatrix} \alpha & 0 \\ 0 & 1 \end{pmatrix} g\right) \text{ 和 } W_0(g) = W_0\left(\begin{pmatrix} \alpha & 0 \\ 0 & 1 \end{pmatrix} g\right).$$

记 W_1 为 W，并记住 W 是依赖于 ψ 之选择的. 这样，上面那个 Fourier 展开就可以改写为

$$F\left(\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} g\right) = W_0(g) + \sum_{A \in K^\times} W\left(\begin{pmatrix} \alpha & 0 \\ 0 & 1 \end{pmatrix} g\right) \psi(\alpha x), \quad x \in A_K.$$

容易验证

$$W\left(\begin{pmatrix}1 & x\\0 & 1\end{pmatrix}g\right)=\psi(x)W(g).$$

我们称这个函数 W 为 F 关于 ψ 的 **Whittaker 函数**. 下面我们概述一下它的性质. 显然, W 是右 $\mathcal{K}$ 有限的. 由于在左边模去一个幂幺元后, 我们总可以把 $\mathrm{GL}_2(A_K)$ 中的元素 g 写作

$$\begin{pmatrix}y & 0\\0 & 1\end{pmatrix}kz$$

的形式, 其中 $y\in I_K$, $k\in\mathcal{K}$, $z\in\mathcal{Z}(A_K)$. 这样, 在有限位 v 处, 如果 F 在 $\mathcal{K}_v=\mathrm{GL}_2(\mathcal{O}_v)$ 的右作用下不变, 那么对任意的 $t\in\mathcal{O}_v$ 有

$$\begin{aligned}W\left(\begin{pmatrix}\alpha & 0\\0 & 1\end{pmatrix}g\right)&=W\left(\begin{pmatrix}\alpha & 0\\0 & 1\end{pmatrix}g\begin{pmatrix}1 & t\\0 & 1\end{pmatrix}\right)\\&=W\left(\begin{pmatrix}\alpha & 0\\0 & 1\end{pmatrix}\begin{pmatrix}y & 0\\0 & 1\end{pmatrix}\begin{pmatrix}1 & t\\0 & 1\end{pmatrix}kz\right)\\&=W\left(\begin{pmatrix}1 & \alpha yt\\0 & 1\end{pmatrix}\begin{pmatrix}\alpha & 0\\0 & 1\end{pmatrix}g\right)\\&=\psi(\alpha yt)W\left(\begin{pmatrix}\alpha & 0\\0 & 1\end{pmatrix}g\right).\end{aligned}$$

由于 ψ_v 的阶是使 ψ_v 在 $\mathfrak{p}_v^{-n}$ 上平凡的最大整数 n, 于是, 从

$$W\left(\begin{pmatrix}\alpha & 0\\0 & 1\end{pmatrix}g\right)\neq 0$$

可以推出 $\mathrm{ord}_v\alpha y\geq-\mathrm{ord}_p\psi_v$. 特别地, 当 $K=\mathbf{Q}$ 时, 我们可取 ψ 是 $A_{\mathbf{Q}}/\mathbf{Q}$ 的标准加法特征标, 即在所有有限位 v 处, ψ_v 的阶均为 0. 这样为了了解 F 在尖点 "i∞" 处的 Fourier 展开, 取

$$g=\left(\begin{pmatrix}y & 0\\0 & 1\end{pmatrix}g\right)\in\mathrm{GL}_2(\mathbf{R})\subset\mathrm{GL}_2(A_{\mathbf{Q}}).$$

从上面讨论可知, 在所有有限位 v 处, $\mathrm{ord}_p\alpha y\geq 0$. 由此推出 $\alpha\in\mathbf{Z}$, 从而 F 在 i∞ 处的 Fourier 展开是

$$F\left(\begin{pmatrix}1 & x\\0 & 1\end{pmatrix}\begin{pmatrix}y & 0\\0 & 1\end{pmatrix}\right) = W_0\left(\begin{pmatrix}y & 0\\0 & 1\end{pmatrix}\right) + \sum_{n\in\mathbf{Z}\setminus\{0\}} W\left(\begin{pmatrix}n & 0\\0 & 1\end{pmatrix}\begin{pmatrix}y & 0\\0 & 1\end{pmatrix}\right)\psi(nx).$$

对自守形式 F, 如果它的常数项 Fourier 系数 W_0 是 0, 则称它是**尖点形式**. 今后, 我们用 $\mathcal{A}(\mathrm{GL}_2(A_K),\eta)$ 表示 $\mathrm{GL}_2(A_K)$ 上特征标为 η 的自守形式空间, 以 $\mathcal{A}^0(\mathrm{GL}_2(A_K),\eta)$ 表示 $\mathcal{A}(\mathrm{GL}_2(A_K),\eta)$ 中由尖点形式组成的子空间.

习题 5 设 $F\in\mathcal{A}(\mathrm{GL}_2(A_{\mathbf{Q}}),\eta)$, 证明 $F\in\mathcal{A}^0(\mathrm{GL}_2(A_{\mathbf{Q}}),\eta)$ 的充分必要条件是:

$$\int_{\mathbf{Q}\setminus A_{\mathbf{Q}}} F\left(\begin{pmatrix}1 & x\\0 & 1\end{pmatrix}g\right)\mathrm{d}x = 0,\quad g\in\mathrm{GL}_2(\mathbf{Q}),$$

其中 $\mathrm{d}x$ 是 $A_{\mathbf{Q}}$ 上使 $A_{\mathbf{Q}}/\mathbf{Q}$ 体积为 1 的 Haar 测度.

在一个有限位 v 处, 取定局部单值化元素 ϖ_v, 用 H_v 表示双陪集

$$\mathcal{K}_v\begin{pmatrix}\varpi_v & 0\\0 & 1\end{pmatrix}\mathcal{K}_v.$$

利用初等因子定理可知, H_v 是由 $\mathrm{GL}_2(K_v)$ 中那些行列式值落在 $\varpi_v\mathcal{U}_v$ 中的整矩阵组成. 因此 H_v 不依赖于 ϖ_v 的选择, 并且可以表成

$$H_v = \bigcup_{u\in\mathcal{O}_v/\mathfrak{p}_v}\begin{pmatrix}\varpi_v & u\\0 & 1\end{pmatrix}\mathcal{K}_v\bigcup\begin{pmatrix}1 & 0\\0 & \varpi_v\end{pmatrix}\mathcal{K}_v.$$

这是一个右 $\mathcal{K}_v$ 陪集的不交并. 设 χ_v 表示 H_v 的特征函数, 对 $\mathrm{GL}_2(A_K)/\mathcal{K}_v$ 上的函数 ϕ, 定义 **Hecke 算子** $\mathbb{T}_v$ 如下:

$$(\mathbb{T}_v\phi)(g) = \frac{1}{Nv}\int_{H_v}\phi(gh)\mathrm{d}h.$$

如此, 我们就在 $\mathcal{A}(\mathrm{GL}_2(A_K),\eta)$ 上定义了 Hecke 算子 $\mathbb{T}_v$. 设 $F\in\mathcal{A}(\mathrm{GL}_2(A_K),\eta)$, 且 F 在 $\mathcal{K}_v$ 的右作用下不变, 则 $\mathbb{T}_vF$ 也在

$\mathcal{A}(\mathrm{GL}_2(A_K),\eta)$ 中，且 $\mathbb{T}_v F$ 也在 K_v 的右作用下不变. 进一步，我们可以证明

$$(\mathbb{T}_v F)(g) = \frac{1}{\mathrm{N}v}\left[\sum_{u\in\mathcal{O}_v/\mathfrak{p}_v} F\left(g\begin{pmatrix}\varpi_v & u\\ 0 & 1\end{pmatrix}\right) + F\left(g\begin{pmatrix}1 & 0\\ 0 & \varpi_v\end{pmatrix}\right)\right]$$

$$= \frac{1}{\mathrm{N}v}\left[\sum_{u\in\mathcal{O}_v/\mathfrak{p}_v} F\left(g\begin{pmatrix}\varpi_v & u\\ 0 & 1\end{pmatrix}\right)\right.$$

$$\left. + \eta_v(\varpi_v)F\left(g\begin{pmatrix}\varpi_v^{-1} & 0\\ 0 & 1\end{pmatrix}\right)\right].$$

当 $K=\mathbf{Q}$, $v=p$ 时，容易验证，这里 $\mathbb{T}_v$ 的定义同经典模形式论中的 Hecke 算子 $\mathbb{T}_p$ 的定义是一致的.

对本节内容想要有更多了解的读者可以参阅参考文献 [10], [13], [17] 和 [37]. 在讨论 $\mathrm{GL}_2(A_K)$ 上的自守表示理论之前，我们需要了解一些局部表示的知识. 所以在下面两节中，我们将讨论 $\mathrm{GL}_2(F)$ 的表示，其中 F 是个局部域.

§2 F 是非 Archimedes 局部域时 $\mathrm{GL}_2(F)$ 的表示

在这一节中，F 总表示一个非 Archimedes 局部域，它的剩余类域是一个有 q 个元素的有限域，$\mathcal{O}$ 表示 F 的整数环，$\mathfrak{p}$ 是 $\mathcal{O}$ 中唯一的极大理想，ϖ 是 $\mathcal{O}$ 的局部单值化元素，从而 $\mathfrak{p}=\varpi\mathcal{O}$. 又记 $\mathcal{U}$ 是 $\mathcal{O}$ 的单位群. 取 F 的一个赋值 $|\ |$, 它在 $\mathcal{U}$ 上平凡且

$$|\varpi| = q^{-1}.$$

设 V 是一个赋予离散拓扑的有限维或无限维复向量空间，$\mathrm{GL}(V)$ 是 V 的可逆线性变换群. $\mathrm{GL}_2(F)$ 到 $\mathrm{GL}(V)$ 的同态映射 π 称为 $\mathrm{GL}_2(F)$ 的一个**复表示**. V 的维数定义为表示 π 的**维数**. 对表示 π, 如果有

(1) 对任意的 $v \in V$, v 在 $\mathrm{GL}_2(F)$ 中的稳定子群是开子群，换句话说，表示 π 诱导出一个从 $\mathrm{GL}_2(F) \times V$ 到 V 的连续映射，则我们称该表示 π 是**光滑的**.

对一个光滑表示 π, 如果有

(2) 对 $\mathrm{GL}_2(\mathcal{O})$ 的任意开子群 H, 空间

$$V^H = \{v \in V: \text{对所有的 } h \in H, \pi(h)v = v\}$$

是有限维的，则我们称该表示 π 是**可容许的**(admissible).

此外，对 $\mathrm{GL}_2(F)$ 的一个表示，如果只有 $\{0\}$ 和 V 是 V 中 $\mathrm{GL}_2(F)$ 的不变子空间，则称这个表示是**不可约的**.

下面我们将研究 $\mathrm{GL}_2(F)$ 的可容许不可约表示.

设 π 是 $\mathrm{GL}_2(F)$ 的一个可容许不可约表示，利用 Schur 引理可知，π 在 $\mathrm{GL}_2(F)$ 的中心 $Z(F)$ 上的限制可以由 F 的一个拟特征标 η 给出，即对任意的 $a \in F$,

$$\pi\left(\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}\right) = \eta(a)\mathrm{id}.$$

我们称这个拟特征标 η 为表示 π 的**中心特征标**. 进一步，我们可以证明表示 π 或者是一维的或者是无限维的. 若 π 是一维的，则存在 F 一个拟特征标 χ, 使得 π 可由

$$\pi(g) = \chi(\det(g)), \quad g \in \mathrm{GL}_2(F)$$

给出. 这样在本节的剩余部分里，我们将专注于 $\mathrm{GL}_2(F)$ 的无限维可容许不可约表示，并在不妨碍理解时把它们简称为**表示**.

对这样一个表示 π, 通常可以建立两个模型 (model), 分别称为 **Kirillov 模型** $\mathfrak{K}_\pi$ 和 **Whittaker 模型** $\mathfrak{W}_\pi$. 它们都是一些函数构成的空间. 粗略地讲，空间 $\mathfrak{K}_\pi$ 的结构简单一些，而 $\mathfrak{W}_\pi$ 的结构则要复杂一些; 不过 $\mathrm{GL}_2(F)$ 的作用则是在 $\mathfrak{K}_\pi$ 上复杂而在 $\mathfrak{W}_\pi$ 上简单. 这两个模型各有各的长处，可以适应我们的不同的需要.

首先，我们来谈谈 Kirillov 模型 $\mathfrak{K}_\pi$. $F^\times$ 上的 Schwartz 函数是 $F^\times$ 上有紧支集的局部常值函数，我们用 $S(F^\times)$ 来表示 $F^\times$ 上

的 Schwartz 函数空间. 又用 w 表示 $\mathrm{GL}_2(F)$ 中的 Weyl 元

$$w = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

空间 $\mathfrak{K}_\pi$ 是由 $\mathcal{S}(F^\times)$ 和 $\mathcal{S}(F^\times)$ 在 $\pi(w)$ 作用下的像生成的. 因此, $\mathfrak{K}_\pi$ 中的函数在 F 上是局部常值的, 并且它的支集包含在 F 的某个紧子集中. 给定 F 的一个阶为 0 的非平凡加法特征标 ψ, $\mathrm{GL}_2(F)$ 的 Borel 子群

$$B(F) = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in \mathrm{GL}_2(F) \right\}$$

在 $\mathfrak{K}_\pi = \mathfrak{K}_\pi(\psi)$ 上的作用可以很容易地描述:

(I) 对任意的 $v \in \mathfrak{K}_\pi$,

$$\left(\pi\left(\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}\begin{pmatrix} z & 0 \\ 0 & z \end{pmatrix}\begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix}\right)v\right)(t) = \eta(z)\psi(xt)v(at),$$

其中 $x \in F$, $z, a, t \in F^\times$, η 是表示 π 的中心特征标.

显然, 上述作用仅依赖于 F 的加法特征标 ψ 和 π 的中心特征标 η. 由于 $\mathrm{GL}_2(F)$ 是由 $B(F)$ 和 Weyl 元 w 生成的, 所以要想对表示 π 有一个清楚的了解, 只需搞清 $\pi(w)$ 的作用. 为此先做些准备. 我们知道

$$F^\times = \bigcup_{n \in \mathbf{Z}} \mathcal{U}\varpi^n,$$

且在每个开子集 $\mathcal{U}\varpi^n$ 上, 局部常值函数一定是 $\mathcal{U}$ 上特征标的线性组合. 设 U 是一个不定元. 如果我们把 $\mathcal{U}$ 的特征标同 $F^\times$ 的在 ϖ 上平凡的特征标等同起来, 那么, 对 $\mathcal{U}$ 的一个特征标 χ, 我们就可以定义 $F^\times$ 上的函数 χU^n,

$$\chi U^n(t) = \begin{cases} \chi(t), & 若\ \mathrm{ord}\ t = n, \\ 0, & 其他情况. \end{cases}$$

从而 $\mathcal{S}(F^\times)$ 中的函数可以写成 χU^n 的线性组合. 于是 $\mathfrak{K}_\pi$ 中的函数就可以用形式线性组合 $\sum\limits_{n,\chi} C_{n,\chi}\chi U^n$ 来表示. 其中, 对每个固

定的 n, 非零的 $C_{n,\chi}$ 的数目有限；并且存在 M, 当 $n < M$ 时, $C_{n,\chi} = 0$. 事实上, 这个 M 与表示 π 有关. 由于表示 π 是由 $\pi(w)$ 在 $\mathcal{S}(F^\times)$ 上的作用所定, 所以它被 $\pi(w)\chi U^0 (\chi \in \widehat{\mathcal{U}})$ 所决定. 设 η_0 是中心特征标 η 在 $\mathcal{U}$ 上的限制. 命

$$v = \pi(w)\chi U^0.$$

从关系

$$\begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix} w = w \begin{pmatrix} 1 & 0 \\ 0 & a \end{pmatrix} = w \begin{pmatrix} a^{-1} & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$$

得

$$v(tu) = (\eta_0 \chi^{-1})(u) v(t), \qquad u \in \mathcal{U},\ t \in F^\times.$$

换句话说, 在每个开集 $\mathcal{U}\varpi^m$ 上, v 是 $\eta_0\chi^{-1}U^m$ 的常数倍. 记这个常数为 $\gamma_m(\eta_0^{-1}\chi, \psi)$. 设 $\gamma(\eta_0^{-1}\chi, \psi, U)$ 是由这些常数定义的 U 的形式 Laurent 级数:

$$\gamma(\eta_0^{-1}\chi, \psi, U) = \sum_{m \in \mathbf{Z}} \gamma_m(\eta_0^{-1}\chi, \psi) U^m.$$

从而

(II) $\pi(w)\chi U^0 = \eta_0 \chi^{-1} \gamma(\eta_0^{-1}\chi, \psi, U)$.

这是利用 $\mathrm{GL}_2(F)$ 的生成元来分析 π 的一种方法, 所以 π 必须遵守一些限制. 从定义可以看到大多数的条件均得到满足, 但还有两个从

$$w^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \text{ 和 } \left(\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} w \right)^3 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

产生的下述两个关键性的关系式:

(A) $\pi(w)^2 = \eta(-1)$;

(B) $$\pi(w)\pi\left(\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\right)\pi(w) = \eta(-1)\pi\left(\begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}\right)\pi(w)\pi\left(\begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}\right).$$

把 (B) 式换成下面关系式 (B′)

$$(\mathrm{B}')\quad \pi(w)\left[\pi\left(\begin{pmatrix}1&1\\0&1\end{pmatrix}\right)\pi(w)-\pi(w)\right]+\eta(-1)$$

$$=\eta(-1)\left[\pi\left(\begin{pmatrix}1&-1\\0&1\end{pmatrix}\right)\pi(w)-\pi(w)\right]\pi\left(\begin{pmatrix}1&-1\\0&1\end{pmatrix}\right)$$

$$+\eta(-1)\pi(w)\pi\left(\begin{pmatrix}1&-1\\0&1\end{pmatrix}\right).$$

可以验证，关系式 (A) 和 (B) 等价于 (A) 和 (B′) 式. (B′) 式的优点在于每个括号里的算子均映空间 $\mathcal{S}(F^\times)$ 为 $\mathcal{S}(F^\times)$, 而 w 在 $\mathcal{S}(F^\times)$ 上的作用可以精确地给出. (A) 和 (B′) 式给出了关于 γ 的一些等式关系. 为了更好地表述这些关系，设 α 是 $F^\times$ 的一个拟特征标， α_0 是 α 在 $\mathcal{U}$ 上的限制，命

$$\gamma(\alpha,\psi,U)=\sum_{m\in\mathbf{Z}}\gamma_m(\alpha_0,\psi)\alpha(\varpi)^m U^m$$

$$=\gamma(\alpha_0,\psi,\alpha(\varpi)U).$$

定义 Γ 函数

$$\Gamma(\alpha,\psi,U)=\sum_{n\in\mathbf{Z}}\Gamma_n(\alpha,\psi)U^n,$$

其中

$$\Gamma_n(\alpha,\psi)=\int_{\mathcal{U}\varpi^n}\alpha(x)\psi(x)\mathrm{d}^\times x,$$

这里 $\mathrm{d}^\times x$ 是使得 $\mathcal{U}$ 之体积为 1 的 $F^\times$ 上的 Haar 测度. 显然

$$\Gamma(\alpha,\psi,U)=\Gamma(\alpha_0,\psi,\alpha(\varpi)U).$$

习题 6　证明：当 α 分歧时， $\Gamma(\alpha,\psi,U)$ 是 U 的单项式；当 α 非分歧时， $\Gamma(\alpha,\psi,U)$ 则是 U 的一个有一个单极点的有理函数.

注　Γ 函数 $\Gamma(\alpha,\psi,U)$ 可视为有限域上的 Gauss 和在 p-adic 域上的推广，因为它是乘法特征标 α 对加法特征标 ψ 的 Fourier 变换. 另外，古典的 Γ 函数 $\Gamma(s)$ 可看成在正实数群上乘法特征标

$t\mapsto t^s$ 对加法特征标 $t\mapsto e^{-t}$ 的 Fourier 变换. 因此, 函数 $\Gamma(\alpha,\psi,U)$ 也是古典的 Γ 函数 $\Gamma(s)$ 在 p-adic 域上的推广.

从等式 (A) 可得

补元公式 (CF)　$\gamma(\chi,\psi,U)\gamma(\eta^{-1}\chi^{-1},\psi,U^{-1})=\eta(-1)$.

而从等式 (B′) 则可以得到

乘法公式 (MF)　任给 $F^\times$ 的两个拟特征标 α 和 β, 存在正整数 $M(\alpha,\beta,\gamma)$, 使得对所有整数 $M\geq M(\alpha,\beta,\gamma)$, 作为 A 和 B 的形式幂级数有下面等式成立:

$$\begin{aligned}&\sum_{\chi\in\widehat{\mathcal{U}},\mathrm{cond}\,\chi\leq M}\{\text{ 常数}\}_U\{\Gamma(\alpha\chi^{-1},\psi,AU^{-1})\Gamma(\beta\chi^{-1},\psi,BU^{-1})\gamma(\chi,\psi,U)\}\\&=(\alpha\beta\eta)(-1)\Gamma(\alpha^{-1}\beta^{-1}\eta^{-1},\psi,A^{-1}B^{-1})\gamma(\alpha,\psi,A)\gamma(\beta,\psi,B)\\&\quad+\begin{cases}0, & \alpha\beta\eta\text{ 是分歧的},\\ \displaystyle\sum_{n\geq -M}(\alpha\beta\eta)(\varpi)^nA^nB^n, & \alpha\beta\eta\text{ 是非分歧的},\end{cases}\end{aligned}$$

其中 “$\{$ 常数 $\}_U\{\cdots\}$” 是指 $\{\cdots\}$ 中 U^0 项的系数.

习题 7　验证补元公式 (CF) 与乘积公式 (MF).

我们将上面的讨论总结为

定理 1(Kirillov 模型的存在性[17],[24])　设 π 是 $\mathrm{GL}_2(F)$ 的具有中心特征标 η 的无限维可容许不可约表示. 任意给定 F 的一个非平凡加法特征 ψ, 均存在一个由支集含于 F 的某个紧子集中的 $F^\times$ 上的局部常值复函数组成的空间 $\mathfrak{K}_\pi(\psi)$. 表示 π 由它在 $\mathfrak{K}_\pi(\psi)$ 上的作用所决定. 空间 $\mathfrak{K}_\pi(\psi)$ 包含了 $F^\times$ 上的 Schwartz 函数空间 $\mathcal{S}(F^\times)$. Borel 子群 $B(F)$ 以 (I) 方式作用于 $\mathfrak{K}_\pi(\psi)$, Weyl 元 w 则以 (II) 方式作用于 $\mathfrak{K}_\pi(\psi)$ 上, 并且在 (II) 中出现的 γ 函数满足 (MF). 更精确一些, 空间 $\mathfrak{K}_\pi(\psi)$ 由空间 $\mathcal{S}(F^\times)$ 和 $\pi(w)\mathcal{S}(F^\times)$ 中的函数张成.

为了以示区别, 我们将用 γ_π 来说明是表示 π 所结合的 γ 函数. (MF) 包含了大量有关 γ_π 的信息. 在此我们介绍其中的一部分.

定理 2[14] 对 $F^\times$ 的任意一个拟特征标 α, 设 α_0 是 α 在 $\mathcal{U}$ 上的限制, 又命

$$\gamma(\alpha, \psi, U) = \gamma(\alpha_0, \psi, \alpha(\varpi)U)$$

是变数为 U 的 Laurent 级数. 假设存在 $F^\times$ 的一个拟特征标 η, 使得 (MF) 成立. 则

(1) γ 满足 (CF);

(2) 或者存在满足 $\mu\nu = \eta$ 的 $F^\times$ 的拟特征标 μ 和 ν, 使得对 $F^\times$ 的任意拟特征标 α, 有

$$\gamma(\alpha, \psi, U) = (q-1)^2 q^{-2} \Gamma(\alpha\mu, \psi, q^{-1/2}U)\Gamma(\alpha\nu, \psi, q^{-1/2}U).$$

或者对 $F^\times$ 的任意拟特征标 α, $\gamma(\alpha, \psi, U)$ 是一个次数不超过

$$\min\{-2, -1 - \mathrm{cond}\alpha^2\eta\}$$

的单项式;

(3) (γ 的扭曲性质) 以 r 表示 $\gamma(1, \psi, U)$ 中 U 的最低次幂, 则对 $F^\times$ 的任意一个满足 $\mathrm{cond}\,\alpha \geq -r$ 的拟特征标 α, 有

$$\gamma(\alpha, \psi, U) = (q-1)^2 q^{-2} \Gamma(\alpha, \psi, q^{-1/2}U)\Gamma(\alpha\eta, \psi, q^{-1/2}U).$$

作为上述三个结论的推论, 我们有

推论 1[14] 出现于 γ 所满足的 (MF) 中的拟特征标 η 是唯一的.

以 $\mathcal{A}(F^\times)$ 表示 $F^\times$ 的拟特征标群. 在 $\mathcal{A}(F^\times)$ 上赋于解析结构, 使得它的每个连通分支均同构于 $\mathbf{C}^\times$, 这里, 连通分支是由在 $\mathcal{U}$ 上取值相同的拟特征标组成. 从而连通分支可以用 $\mathcal{U}$ 的特征标来参数化. 用 $\gamma(\alpha, \psi)$ 表示 $\gamma(\alpha, \psi, 1)$. 固定 ψ, 将 γ 视为 $\mathcal{A}(F^\times)$ 上的函数. 定理 2(2) 告诉我们: γ 是 $\mathcal{A}(F^\times)$ 上的一个有理函数, 并且在某个 $\mathcal{A}(F^\times)$ 的连通分支上它是一个至多有两个极点的有理函数, 而在其他连通分支上则是一个单项式. 因此它不是全纯函数的充要条件是: 它为两个 Γ 函数的积. 此时, 在 $\mu\nu^{-1} \neq |\ |^{\pm 1}$ 时, 它

有两个极点；当 $\mu\nu^{-1} = |\ |^{\pm 1}$ 时，它有一个极点，这里 μ 和 ν 与定理 2(2) 中的 μ 和 ν 相同.

下面这个定理是说函数 γ 事实上决定一个表示，而它又由 (MF) 确定.

定理 3[24],[14]　*对 $\mathcal{A}(F^\times)$ 上的一个有理函数*

$$\gamma(\alpha, \psi, U) = \gamma(\alpha_0, \psi, \alpha(\varpi)U),$$

存在 $\mathrm{GL}_2(F)$ 的一个无限维可容许不可约表示 π，其中心特征标为 η，使得 $\gamma = \gamma_\pi$ 的充要条件是：γ 满足具有特征标 η 的乘法公式 (MF). 此外，γ_π 决定表示 π.

下面概述一下定理的证明. 我们知道 γ_π 满足 (MF). 反过来，给出 $\mathcal{A}(F^\times)$ 上一个满足 (MF) 的有理函数 γ，我们希望可以利用 Kirillov 模型 $\mathfrak{K}_\pi$ 来构造一个表示. 由于 Borel 子群的作用是由 (I) 给出的，所以问题的关键在于给出 Weyl 元 w 在 Schwartz 空间 $\mathcal{S}(F^\times)$ 上的作用. 当然，我们要用 (II) 来定义 w 的作用. 研究发现，当 γ 是个单项式时，$\pi(w)$ 映空间 $\mathcal{S}(F^\times)$ 为 $\mathcal{S}(F^\times)$，进而

$$\mathfrak{K}_\pi = \mathcal{S}(F^\times);$$

当 γ 是两个 Γ 函数的积时，按照 γ 有两个还是一个极点，$\mathcal{S}(F^\times)$ 在

$$\mathfrak{K}_\pi = \mathcal{S}(F^\times) + \pi(w)\mathcal{S}(F^\times)$$

中的指数或者是 2 或者为 1. 因为公式 (CF) 和 (MF) 可以确定关系式 (A) 和 (B′)，所以上面定义的作用能进一步扩展为 $\mathrm{GL}_2(F)$ 的作用. 从而就给出了 $\mathrm{GL}_2(F)$ 的一个表示.

这个证明导致下面的关于 $\mathrm{GL}_2(F)$ 的无限维可容许不可约表示 π 的分类：按照 $\mathcal{S}(F^\times)$ 在 $\mathfrak{K}_\pi$ 中的余维数是 2, 1 还是 0，我们分别称表示 π 是**主序列表示**，**极点**、**特殊表示**和**超尖点表示**. 相应地，γ_π 在 $\mathcal{A}(F^\times)$ 中分别有两个、一个和零个极点. 在前面两种情况下，存在拟特征标 μ 和 ν，使得

$$\gamma_\pi(\alpha, \psi) = (q-1)^2 q^{-2}\Gamma(\alpha\mu, \psi, q^{-1/2})\Gamma(\alpha\nu, \psi, q^{-1/2}).$$

当然，第一种情况要求

$$\mu\nu^{-1} \neq |\ |^{\pm 1},$$

而后者则要求

$$\mu\nu^{-1} = |\ |^{\pm 1}.$$

给定 μ 和 ν, 我们用

$$\tau\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} = \mu(a)\nu(d)\left|\frac{a}{d}\right|^{1/2}$$

来定义 $B(F)$ 的一个拟特征标 τ. 由 τ 诱导出 $\mathrm{GL}_2(F)$ 的一个表示 $\rho(\mu,\nu)$, 可以证明表示 π 也可以由表示 $\rho(\mu,\nu)$ 得到. Jacquet 和 Langlands[17] 证明了，当 $\mu\nu^{-1} \neq |\ |^{\pm 1}$ 时，表示 $\rho(\mu,\nu)$ 是不可约的，记作 $\pi(\mu,\nu)$; 当 $\mu\nu^{-1} = |\ |^{\pm 1}$ 时，表示 $\rho(\mu,\nu)$ 是由一个无限维表示 $\sigma(\mu,\nu)$ 和一个一维表示构成的，并且这个无限维表示 $\sigma(\mu,\nu)$ 是唯一的. 他们还证明了，表示 $\pi(\mu,\nu)$ 或 $\sigma(\mu,\nu)$ 的 γ 因子就是上面的 γ_π. 于是，我们可以直接证明 (参阅参考文献 [14]), 对任意给出的 $F^\times$ 的两个拟特征标 μ 和 ν, 由

$$\gamma(\alpha,\psi) = (q-1)^2q^2\Gamma(\alpha\mu,\psi,q^{-1/2})\Gamma(\alpha\nu,\psi,q^{-1/2})$$

定义出的 $S(F^\times)$ 上函数满足特征标 $\eta = \mu\nu$ 的乘法公式 (MF). 于是，从 μ 和 ν 就诱导出一个主序列表示，或者特殊表示. 此外，Carayol[6] 和 Kutzko[19,20] 证明了超尖点表示也可以通过一个诱导过程构造出来. 不过，这一过程借助的不再是 Borel 子群，而是一些紧模中心子群.

事实上，对 F 的任意非平凡加法特征标 ϕ, 表示 π 的 Kirillov 模型 $\mathfrak{K}_\pi(\phi)$ 都是存在的. 设 ψ 是一个阶为 0 的加法特征标，$\phi = \psi^t$, 则 $\mathrm{ord}\ \psi^t = \mathrm{ord}\ t$, 并且

$$\gamma_\pi(\chi,\psi^t,U) = q^{-\mathrm{ord}\,t}(\eta^{-1}\chi^{-2})(t)\gamma_\pi(\chi,\psi,U)U^{-2\mathrm{ord}\,t}.$$

接下来讨论 π 的 Whittaker 模型. 设 ψ 是 F 的一个非平凡加法特征标，$\mathfrak{K}_\pi = \mathfrak{K}_\pi(\psi)$ 是表示 π 的 Kirillov 模型. 任取 $v \in \mathfrak{K}_\pi$,

定义 $\mathrm{GL}_2(F)$ 的一个 Whittaker 函数 W_v 为

$$W_v(g) = (\pi(g)v)(1), \quad g \in \mathrm{GL}_2(F).$$

命 $\mathfrak{W}_\pi = \mathfrak{W}_\pi(\psi) = \{W_v : v \in \mathfrak{K}_\pi(\psi)\}$. 以右平移方式在 $\mathfrak{W}_\pi$ 上定义 $\mathrm{GL}_2(F)$ 的一个作用 π'. 即对 $g' \in \mathrm{GL}_2(F)$,

$$\begin{aligned}(\pi'(g')W_v)(g) &= W_v(gg') = (\pi(gg')v)(1) \\ &= (\pi(g)(\pi(g')v))(1) = W_{\pi(g')v}(g).\end{aligned}$$

这表明 π' 等价于 π. 我们称空间 $(\pi, \mathfrak{W}_\pi(\psi))$ 为表示 π 的 **Whittaker 模型**. 我们也可以发现 Whittaker 函数 W_v 满足下面关系

$$\begin{aligned}W_v\left(\begin{pmatrix}1 & x\\ 0 & 1\end{pmatrix} g\right) &= \left(\pi\begin{pmatrix}1 & x\\ 0 & 1\end{pmatrix}\pi(g)v\right)(1) \\ &= \psi(x)(\pi(g)v)(1) = \psi(x)W_v(g),\end{aligned}$$

$$W_v\left(\begin{pmatrix}z & 0\\ 0 & z\end{pmatrix} g\right) = \eta(z)W_v(g),$$

以及

$$W_v\left(\begin{pmatrix}a & 0\\ 0 & 1\end{pmatrix}\right) = v(a),$$

其中 $x \in F$, $z \in F^\times$, $g \in \mathrm{GL}_2(F)$.

设 ν 是 $F^\times$ 的一个拟特征标, 我们知道 ν 结合的局部 L-函数是

$$L(\pi, U) = \begin{cases}(1-\mu(\varpi)U)^{-1}, & \mu \text{ 是非分歧的}, \\ 1, & \mu \text{ 是分歧的}.\end{cases}$$

对 $\mathrm{GL}_2(F)$ 的表示 π, 定义它结合的 L-函数为

$$L(\pi, U) = \begin{cases}L(\mu, U)L(\nu, U), & \pi = \pi(\mu, \nu) \text{ 是主序列表示}; \\ L(\mu, U), & \pi = \sigma(\mu, \nu) \text{ 是特殊表示 } (\mu\nu^{-1} = |\ |); \\ 1, & \pi \text{ 是超尖点表示}.\end{cases}$$

对 Whittaker 函数 $W \in \mathfrak{W}_\pi(\psi)$ 和 $g \in \mathrm{GL}_2(F)$, 定义两个如下形式幂级数

$$\Phi(g,U,W)=\int_{F^\times}W\left(\begin{pmatrix}a&0\\0&1\end{pmatrix}g\right)|a|^{-1/2}U^{\mathrm{ord}\,a}\mathrm{d}^\times a$$

和

$$\widetilde{\Phi}(g,U,W)=\int_{F^\times}W\left(\begin{pmatrix}a&0\\0&1\end{pmatrix}g\right)|a|^{-1/2}\eta(a)^{-1}U^{\mathrm{ord}\,a}\mathrm{d}^\times a.$$

它们在 U 的绝对值很小时是收敛的. 由于 $\mathrm{GL}_2(F)$ 对 Whittaker 函数的作用是右平移的, 所以, 我们只需就某个 $g\in\mathrm{GL}_2(F)$ 研究 $\Phi(g,U,W)$ 和 $\widetilde{\Phi}(g,U,W)$ 即可, 其中 W 跑遍空间 $\mathfrak{W}_\pi(\psi)$.

下面看几个例子. 对 $v=\chi U^m\in\mathcal{S}(F^\times)$, 取 $W=W_v$, 则

$$\Phi(\mathrm{id},U,W_v)=\begin{cases}q^{m/2}U^m, & \chi\text{ 是非分歧的},\\ 0, & \chi\text{ 是分歧的};\end{cases}$$

及

$$\widetilde{\Phi}(w,U,W_v)=\begin{cases}q^{m/2}U^{-m}\gamma_\pi(\eta^{-1},\psi,q^{1/2}U), & \chi\text{ 是非分歧的},\\ 0, & \chi\text{ 是分歧的}.\end{cases}$$

此外, 若 π 是主序列表示 $\pi(\mu,\nu)$ 或特殊表示 $\sigma(\mu,\nu)$ 时, 对 $v=\pi(w)\chi U^0$ 有

$$\Phi(\mathrm{id},U,W_v)=\begin{cases}\gamma_\pi(\chi_0,\psi,q^{1/2}U), & \mu\text{ 是非分歧的 }(\chi_0\text{ 是平凡特征标}),\\ 0, & \mu\text{ 是分歧的};\end{cases}$$

及

$$\widetilde{\Phi}(w,U,W_v)=\begin{cases}\eta(-1), & \mu\text{ 是非分歧的},\\ 0, & \mu\text{ 是分歧的}.\end{cases}$$

可以证明, 对任意的 $g\in\mathrm{GL}_2(F)$ 和 $W\in\mathfrak{W}_\pi$, $\Phi(g,U,W)/L(\pi,U)$ 是 U 之方幂的线性组合, 由此得到 $\Phi(g,U,W)$ 的一个解析开拓. 更进一步, 如果我们把 $\Phi(g,U,W)$ 写作 U 的有理函数的形式, 则 $L(\pi,U)$ 是这些 $\Phi(g,U,W)$ 的分母的"最小公倍式".

接下来定义表示 π 的逆步表示 $\widetilde{\pi}$. 设 V 是 π 的表示空间, $V^\vee$ 是 V 上的线性泛函空间. 于是存在一个配对

$$\langle\, ,\, \rangle : V \times V^\vee \longrightarrow \mathbf{C},$$
$$(v, v^\vee) \longmapsto \langle v, v^\vee \rangle = v^\vee(v).$$

因此

$$\langle v, \pi^*(g)v^\vee \rangle = \langle \pi(g^{-1})v, v^\vee \rangle$$

就定义了一个 $\mathrm{GL}_2(F)$ 在 $V^\vee$ 上的作用 π^*. 若 V 是有限维的话, 则

$$\pi^*(g) = {}^t(\pi(g^{-1})) = {}^t\pi(g)^{-1}.$$

从而 π^* 为 π 的逆步表示. 不过遗憾的是, 在这里 V 是无限维的, 此时 π^* 通常不是可容许的, 这样逆步表示就不是 π^*. 为了得到一个可容许表示, 考虑由 $V^\vee$ 的光滑对偶构成的子空间 $\widetilde{V}$, 它是由

$$\int_S \pi^*(g)v^\vee \mathrm{d}g, \quad v^\vee \in V^\vee$$

这样的泛函生成的, 其中 S 跑遍 $\mathrm{GL}_2(F)$ 的所有紧开子集. 于是 $\widetilde{V}$ 在 $\pi^*(\mathrm{GL}_2(F))$ 的作用下不变, 并且在 π 是可容许不可约时, 该作用亦为可容许不可约的, 称此表示 $\widetilde{\pi}$ 为表示 π 的**逆步表示**. 设 η 是表示 π 的中心特征标, 则 $\widetilde{\pi}$ 同构于 $\pi \bigotimes \eta^{-1}$, 且

$$\gamma_{\widetilde{\pi}}(\chi, \psi, U) = \gamma_\pi(\chi\eta^{-1}, \psi, U),$$
$$\mathfrak{W}_{\widetilde{\pi}} = \mathfrak{W}_\pi \bigotimes (\eta^{-1} \circ \det).$$

特别地, 当 $\pi = \pi(\mu, \nu)$ 或 $\sigma(\mu, \nu)$ 时,

$$\widetilde{\pi} = \pi(\nu^{-1}, \mu^{-1}) \text{ 或 } \sigma(\nu^{-1}, \mu^{-1}).$$

从上面定义我们得到

$$L(\widetilde{\pi}, U) = \begin{cases} L(\mu^{-1}, U)L(\nu^{-1}, U), & \pi = \pi(\mu, \nu), \\ L(\nu^{-1}, U), & \pi = \sigma(\mu, \nu)\ (\mu\nu^{-1} = |\,|), \\ 1, & \pi \text{ 是超尖点的}. \end{cases}$$

命

$$\varepsilon(\pi,\psi,U)=\gamma_\pi(\eta^{-1},\psi,q^{-1/2}U^{-1})\frac{L(\pi,U)}{L(\widetilde{\pi},q^{-1}U^{-1})}.$$

可以证明 $\varepsilon(\pi,\psi,U)$ 是 U 的一个单项式.

注意到, 存在 $W'\in\mathfrak{W}_\pi\bigotimes(\eta^{-1}\circ\det)$, 即 W' 在 $\widetilde{\pi}$ 的 Whittaker 模型里, 使得有

$$\widetilde{\Phi}(g,U,W)=\Phi(g,U,W').$$

于是对 $\widetilde{\Phi}(g,U,W)/L(\widetilde{\pi},U)$ 也有同样的结论成立. 利用补元公式

$$\gamma_\pi(\chi_0,\psi,q^{1/2}U)\gamma_\pi(\eta^{-1},\psi,q^{-1/2}U^{-1})=\eta(-1),$$

并结合上面的计算, 可以证明函数

$$\Phi(g,U,W)/L(\pi,U)\quad 和\quad \widetilde{\Phi}(wg,q^{-1}U^{-1},W)/L(\widetilde{\pi},q^{-1}U^{-1})$$

解析开拓后均有与 W 无关的比率 $\varepsilon(\pi,\psi,U)^{-1}$. 从而我们得到下面结论:

定理 4 (局部函数方程[17]) 设 π 是 $\mathrm{GL}_2(F)$ 的具有中心特征标 η 的无限维不可约可容许表示. 设 $L(\pi,U),L(\widetilde{\pi},U)$ 和 $\varepsilon(\pi,\psi,U)$ 与前面所设一样. 对 π 的任意 Whittaker 函数 $W\in\mathfrak{W}_\pi(\psi)$ 和 $g\in\mathrm{GL}_2(F)$. 如前定义积分 $\Phi(g,U,W)$ 和 $\widetilde{\Phi}(g,U,W)$, 则 $L(\pi,U)^{-1}$(或 $L(\widetilde{\pi},U)^{-1}$) 是常数项为 1 的 U 之多项式, 并且它是所有满足: "对所有的 g,W, 函数 $\Phi(g,U,W)f(U)$(或 $\widetilde{\Phi}(g,U,W)f(U)$) 作为 U 的方幂之线性组合有一个到整个 U 平面上的解析开拓" 的 U 之多项式 $f(U)$ 集合中次数最低的. 进一步, 对任意的 g 和 W, 我们有下面函数方程

$$\frac{\widetilde{\Phi}(wg,q^{-1}U^{-1},W)}{L(\widetilde{\pi},q^{-1}U^{-1})}=\varepsilon(\pi,\psi,U)\frac{\Phi(g,U,W)}{L(\pi,U)}.$$

在本节剩余的部分, 我们将讨论 π 的表示空间 V 中的"新向量", 这是由 P. Deligne 引入的概念, 可以视为局部新形式理论. 读者将会看到这些向量都在 π 的 Kirillov 模型 $\mathfrak{K}_\pi(\psi)$ 中. 以 $n(\psi)$

记 ψ 的阶. 首先我们考虑 $\mathfrak{K}_\pi(\psi)$ 中满足

$$\pi\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right) v = \eta(d)v, \qquad a, d \in \mathcal{U},\ b \in \mathcal{O}$$

的函数 v. 按照由 (I) 描述的 $B(F)$ 对 v 的作用, 上式等于说, 对 $\mathrm{supp}v$ 中任意元 x, $\psi(\mathcal{O}x) = 1$; 以及对任意的 $u \in \mathcal{U}, v(ux) = v(x)$. 于是我们看到 v 的支集含于 $\varpi^{-n(\psi)}\mathcal{O} = \mathfrak{p}^{-n(\psi)}$ 中, 且 $v(x)$ 仅依赖于 x 的阶. 这样的向量有很多, 例如, 设 $m \geq -n(\psi)$, χ_0 为 $\mathcal{U}$ 的平凡特征标, $\chi_0 U^m \in \mathcal{S}(F^\times)$ 就是一个这样的向量. 用 V_0 表示 $\mathfrak{K}_\pi(\psi)$ 中由这些函数构成的空间. 由于 π 是光滑的, 所以对任意的 $v \in V_0$, 存在 $\mathrm{GL}_2(F)$ 的一个开子群. 它在 v 上作用平凡. 特别地, 当 m 充分大时, v 在

$$\begin{pmatrix} 1 & 0 \\ \mathfrak{p}^m & 1 \end{pmatrix}$$

作用下不变. 设 n 是使得存在非零的 $v_0 \in V_0$, 它在

$$\begin{pmatrix} 1 & 0 \\ \mathfrak{p}^n & 1 \end{pmatrix}$$

作用下不变的最小自然数, 并固定 v_0 的选取. 令 G'_n 是由

$$\begin{pmatrix} 1 & 0 \\ \mathfrak{p}^n & 1 \end{pmatrix} \text{ 和 } \begin{pmatrix} 1 & \mathcal{O} \\ 0 & 1 \end{pmatrix}$$

生成的子群, 则

$$G'_n = \begin{cases} \left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathcal{O}) : a-1, d-1, c \in \mathfrak{p}^n\right\}, & n > 0, \\ \mathrm{SL}_2(\mathcal{O}), & n = 0, \\ \mathrm{SL}_2(F), & n < 0. \end{cases}$$

显然 v_0 在 G'_n 作用下不变. 如果 $n < 0$, 由于 $\mathrm{GL}_2(F)v_0$ 张成的空间是由

$$\pi\left(\begin{pmatrix} \varpi^m & 0 \\ 0 & 1 \end{pmatrix}\right) v_0, \quad m \in \mathbf{Z}$$

生成的. 而这是 $\mathfrak{K}_\pi(\psi)$ 中的一个非平凡子空间, 同 π 的不可约性矛盾, 因此 $n \geq 0$. 又由于一方面

$$\left\{\begin{pmatrix} d^{-1} & 0 \\ 0 & d \end{pmatrix} : d \in \mathcal{U}\right\}$$

在 v_0 上的作用是乘以 $\eta(d)$, 另一方面该作用是平凡的, 于是 n 不小于 $\operatorname{cond}\eta$. 当 $k \geq 0$ 时, 定义同余子群

$$G_k = \left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathcal{O}) : c \in \mathfrak{p}^k\right\},$$

且设

$$X_k = \left\{v \in \mathfrak{K}_\pi(\psi) : \text{对任意的} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G_k,\right.$$

$$\left.\pi\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right) v = \eta(d) v\right\}.$$

因此 $v_0 \in X_n$ 且 $X_n \subset X_{n+1} \subset \cdots$ 是 V_0 的一个滤链 (filtration).

定理 5 (Deligne[7]) 空间 X_k 是 $k-n+1$ 维的, 且

$$\left\{\pi\left(\begin{pmatrix} \varpi^{-i} & 0 \\ 0 & 1 \end{pmatrix}\right) v_0 : 0 \leq i \leq k-n\right\}$$

是它的一组基.

证 由 n 的极小性知, 当 $k < n$ 时, $X = \{0\}$. 进而易证, 当 $i \geq 0$ 时,

$$\pi\left(\begin{pmatrix} \varpi^{-i} & 0 \\ 0 & 1 \end{pmatrix}\right) X_k$$

含于 X_{k+1} 中, 并且

$$\pi\left(\begin{pmatrix} \varpi^{-i} & 0 \\ 0 & 1 \end{pmatrix}\right) v_0, \quad i \geq 0$$

是线性无关的. 于是只需证

$$\dim\left(X_k \Big/ \pi\left(\begin{pmatrix} \varpi^{-1} & 0 \\ 0 & 1 \end{pmatrix}\right) X_{k-1}\right) \leq 1.$$

事实上，设 $v_1, v_2 \in X_k - \{0\}$. 则存在不全为 0 的常数 a 和 b, 使得 $av_1 + bv_2$ 的支集位于集合 $\mathfrak{p}^{-n(\psi)+1}$ 中，从而

$$\pi\left(\begin{pmatrix} \varpi & 0 \\ 0 & 1 \end{pmatrix}\right)(av_1 + bv_2) \in V_0$$

且在

$$\begin{pmatrix} 1 & 0 \\ \mathfrak{p}^{k-1} & 1 \end{pmatrix}$$

作用下不变. 当 $k = n$ 时，由 n 的极小性知，$av_1 + bv_2 = 0$. 而当 $k > n$ 时，则有

$$av_1 + bv_2 \in \pi\left(\begin{pmatrix} \varpi^{-1} & 0 \\ 0 & 1 \end{pmatrix}\right) X_{k-1}.$$

由此定理得证.

由定理 5 知，空间 X_n 是一维的，其中的非零向量称为**新向量**. 从上面的证明看到，新向量在 $\mathcal{U}\varpi^{-n(\psi)}$ 上是非 0 的. 整数 n 称为表示 π 之前导子的**指数**. 当 $n = 0$ 时，我们称表示 π 是**非分歧的**或**类一的**. 可设 v_0 是使得 $v_0(\mathcal{U}\varpi^{-n(\psi)}) = 1$ 的正规化新向量.

从前面讨论知道，若记

$$\begin{aligned} H &= \mathrm{GL}_2(\mathcal{O})\begin{pmatrix} \varpi & 0 \\ 0 & 1 \end{pmatrix}\mathrm{GL}_2(\mathcal{O}) \\ &= \bigcup_{u \in \mathcal{O}/\mathfrak{p}} \begin{pmatrix} \varpi & u \\ 0 & 1 \end{pmatrix}\mathrm{GL}_2(\mathcal{O}) \bigcup \begin{pmatrix} 1 & 0 \\ 0 & \varpi \end{pmatrix}\mathrm{GL}_2(\mathcal{O}). \end{aligned}$$

则 π 的 Hecke 算子 $\mathbb{T}$ 在 π 的表示空间 V 上的作用是与 H 的特征函数的 q^{-1} 倍作卷积，即

$$\begin{aligned} \mathbb{T}v = q^{-1}\int_{\mathrm{GL}_2(\mathcal{O})} \Bigg\{ \sum_{u \in \mathcal{O}/\mathfrak{p}} \pi\left(\begin{pmatrix} \varpi & u \\ 0 & 1 \end{pmatrix}\right)\pi(k)v \\ + \pi\left(\begin{pmatrix} 1 & 0 \\ 0 & \varpi \end{pmatrix}\right)\pi(k)v \Bigg\} \mathrm{d}k. \end{aligned}$$

如果 v_0 在 $\mathrm{GL}_2(\mathcal{O})$ 作用下不变, 即 $n=0$, 则 $\mathbb{T}v_0$ 同样也在 $\mathrm{GL}_2(\mathcal{O})$ 作用下不变. 于是存在特征值 λ, 使得 $\mathbb{T}v_0=\lambda v_0$. 此时, v_0 的支集位于 $\mathcal{O}\varpi^{-n(\psi)}$ 中, 且

$$\begin{aligned}\mathbb{T}v_0(x)&=q^{-1}\left[\sum_{u\in\mathcal{O}/\mathfrak{p}}\psi(ux)v_0(\varpi x)+\eta(\varpi)v_0(\varpi^{-1}x)\right]\\&=v_0(\varpi x)+q^{-1}\eta(\varpi)v_0(\varpi^{-1}x),\quad x\in\mathcal{O}\varpi^{-n(\psi)}.\end{aligned}$$

由于 $v_0(x)$ 仅依赖于 x 的阶, 所以由上式可得: 当 $m\geq -n(\psi)$ 时

$$\lambda v_0(\varpi^m)=v_0(\varpi^{m+1})+q^{-1}\eta(\varpi)v_0(\varpi^{m-1});$$

或等价地

$$\begin{aligned}\Phi(\mathrm{id},U,W_{v_0})&=\int_{F^\times}v_0(a)|a|^{-1/2}U^{\mathrm{ord}\,a}\mathrm{d}^\times a\\&=(1-\lambda q^{1/2}U+\eta(\varpi)U^2)^{-1}(q^{1/2}U)^{-n(\psi)}.\end{aligned}$$

利用定理 4, 我们知道, 如果表示 π 是由两个 $F^\times$ 的非分歧拟特征标 μ 和 ν 诱导出的主序列表示 $\pi(\mu,\nu)$, 其中 $\mu\nu=\eta$, 则

$$L(\pi,U)^{-1}=L(\mu,U)^{-1}L(\nu,U)^{-1}=1-\lambda q^{1/2}U+\eta(\varpi)U^2,$$

其中 λ 是 Hecke 算子 $\mathbb{T}$ 关于 π 的一个新向量的特征值. 反过来, 对 $F^\times$ 的两个拟特征标 μ 和 ν, 且 $\mu\nu=\eta$, 假设 $\pi=\pi(\mu,\nu)$ 是一个主序列表示, 我们希望证明 π 的前导子的指数为 0. 为此, 取一个 0 阶加法特征 ψ, 由定理 2(2) 我们明确知道: 函数 $\gamma_\pi(\chi,\psi,U)$, 特别地, $\gamma_\pi(\chi_0,\psi,U)$ 是 U 的一个有理函数, 其分母为

$$(1-\mu(\varpi)q^{-1/2}U)(1-\nu(\varpi)q^{-1/2}U)=1+\alpha U+\eta(\varpi)q^{-1}U^2,$$

其中 $\alpha=-(\mu(\varpi+\nu(\varpi))q^{-1/2}$; 分子为

$$\begin{aligned}&(1+\alpha U+\eta(\varpi)q^{-1}U^2)\gamma_\pi(\chi_0,\psi,U)\\&\quad=q^{-1}U^{-2}[\eta(\varpi)^{-1}+\eta(\varpi)^{-1}q\alpha U+qU^2].\end{aligned}$$

考虑 $\mathfrak{K}_\pi(\psi)$ 中函数

$$v=c_{-2}\chi_0U^{-2}+c_{-1}\chi_0U^{-1}-\eta(\varpi)qc_{-2}\pi(w)\chi_0U^0$$

$$+ (c_{-1} - \alpha q c_{-2})\pi(w)\chi_0 U^{-1},$$

其中 c_{-1}, c_{-2} 为待定常数. 从上面 $\gamma_\pi(\chi_0, \psi, U)$ 的精确表达式和由 (II) 得到的关系

$$\pi(w)\chi_0 U^m = \eta(\varpi)^{-m}\gamma_\pi(\chi_0, \psi, U)U^{-m}$$

知 $\pi(w)v = v$. 进而可以证明 v 的支集在 $\mathfrak{p}^{-1}$ 中. 取一个非 0 常数 c_{-2}, 则存在唯一的 c_{-1}, 使得 v 的支集在 $\mathcal{O}$ 中. 由于向量 $\chi_0 U^{-2}, \chi_0 U^{-1}, \pi(w)\chi_0 U^{-1}$ 和 $\pi(w)\chi_0 U^0$ 是线性无关的, 所以我们可找到一个非零向量 $v \in V_0$, 它在 $\mathrm{SL}_2(\mathcal{O})$ 作用下不变, 从而它是表示 π 的一个新向量, 并且 π 的前导子之指数为 0. 总结上面的讨论, 我们证明了, 表示 π 是一个由 $F^\times$ 的两个非分歧拟特征标 μ 和 ν 诱导出的主序列表示 $\pi(\mu, \nu)$ 的充要条件是: π 是非分歧的. 此时, 存在一个位于 π 的 Whittaker 模型中的正规化新向量 $W_{v_0} \in \mathfrak{W}_\pi(\psi)$, 使得

$$\Phi(\mathrm{id}, U, W_{v_0}) = (q^{1/2}U)^{-n(\psi)}L(\pi, U).$$

下面研究表示 π 分歧, 即 $n = \mathrm{cond}\,\pi > 0$ 时的情况. 令 $v_0 \in \mathfrak{K}_\pi(\psi)$ 是 π 的正规化新向量. 我们已知 $v_0(t)$ 仅依赖于 t 的阶, $\mathrm{supp}\, v_0 \subset \mathfrak{p}^{-n(\psi)}$, 以及 $v_0(\varpi^{-n(\psi)}) = 1$. 考虑函数

$$v = \left(\sum_{\substack{u \in \mathcal{O}/\mathfrak{p} \\ u \notin \mathfrak{p}}} \frac{1}{q-1} \pi\left(\begin{pmatrix} 1 & u\varpi^{-1} \\ 0 & 1 \end{pmatrix} \right) v_0 \right) - v_0.$$

利用 (I) 可以证明

$$v(t) = \begin{cases} -\dfrac{q}{q-1} v_0(t), & t \in \mathcal{U}\varpi^{-n(\psi)}, \\ 0, & \text{其他情况}. \end{cases}$$

从而 $v = a\chi_0 U^{-n(\psi)}$, 其中 $a = -q/(q-1)$. 另一方面, 对 $u \in \mathcal{U}$ 和

$c \in \mathfrak{p}^{n+1}$, 有

$$\begin{pmatrix} 1 & -u\varpi^{-1} \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ c & 1 \end{pmatrix} \begin{pmatrix} 1 & u\varpi^{-1} \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 - cu\varpi^{-1} & -cu^2\varpi^{-2} \\ c & 1 - cu\varpi^{-1} \end{pmatrix} \in G_n'.$$

于是

$$\pi\left(\begin{pmatrix} 1 & 0 \\ \mathfrak{p}^{n+1} & 1 \end{pmatrix}\right) v = v.$$

我们已经证明 $\chi_0 U^{-n(\psi)} \in X_{n+1}$. 从而由定理 5 知, 存在常数 b, 使得

$$\chi_0 U^{-n(\psi)} = v_0 - b\pi\left(\begin{pmatrix} \varpi^{-1} & 0 \\ 0 & 1 \end{pmatrix}\right) v_0.$$

利用上面对 v_0 的讨论, 我们可把它表为

$$v_0 = \sum_{i \geq -n(\psi)} c_i \chi_0 U^i,$$

其中 $c_{-n(\psi)} = 1$. 从而

$$\pi\left(\begin{pmatrix} \varpi^{-1} & 0 \\ 0 & 1 \end{pmatrix}\right) v_0 = \sum_i c_i \chi_0 U^{i+1}.$$

于是, 当 $i > -n(\psi)$ 时, 有 $c_i = b^{i+n(\psi)}$. 若 $b \neq 0$, 则 $\Phi(\mathrm{id}, U, W_{v_0})$ 有一个单极点. 利用定理 4 可以得到, 当 $L(\pi, U) = 1$ 时,

$$v_0 = \chi_0 U^{-n(\psi)},$$

即 $b = 0$. 此时 $\Phi(\mathrm{id}, U, W_{v_0}) = (q^{1/2}U)^{-n(\psi)}$. 反过来, 假设 $v_0 = \chi_0 U^{-n(\psi)}$, 我们希望证明 $L(\pi, U) = 1$. 如若不然, 则 $L(\pi, U)$ 有一个单极点. 由定理 4 前面的讨论知, 存在 Kirillov 函数

$$v = \sum_{i > -\infty} c_i \chi_0 U^i,$$

使得 $\Phi(\mathrm{id},U,W_v)$ 的分母是 $L(\pi,U)^{-1}$. 于是, 对无限多个 i 有 $c_i \neq 0$. 必要时将 v 换成

$$\pi\left(\begin{pmatrix} \varpi^{-m} & 0 \\ 0 & 1 \end{pmatrix}\right) v,$$

并把 m 取得充分大, 我们总可假定 $\mathrm{supp}\, v \subset \mathfrak{p}^{-n(\psi)}$, 即 $v \in V_0$. 由表示 π 的光滑性知, 存在 m, 使得 $v \in X_m$; 另一方面, 由定理 5 知 v 为

$$\pi\left(\begin{pmatrix} \varpi^{-i} & 0 \\ 0 & 1 \end{pmatrix}\right) v_0 = \chi_0 U^{-n(\psi)+i}, \quad 0 \le i \le m-n$$

的线性组合. 由此得到, 当 $i > m-n-n(\psi)$ 时, $c_i = 0$. 故矛盾, 从而 $L(\pi,U) = 1$. 于是, $L(\pi,U)=1$ 的充要条件是

$$v_0 = \chi_0 U^{-n(\psi)},$$

此时

$$\Phi(\mathrm{id},U,W_{v_0}) = (q^{1/2}U)^{-n(\psi)} L(\pi,U).$$

现在还剩下 $L(\pi,U)$ 有一个单极点的情况需要研究. 这时, 我们有

$$v_0 = \sum_{i=0}^{\infty} b^i \chi_0 U^{-n(\psi)+i}$$

和

$$\Phi(\mathrm{id},U,W_{v_0}) = (q^{1/2}U)^{-n(\psi)} L(\pi,U),$$

其中 $L(\pi,U) = (1-bq^{1/2}U)^{-1}$. 上面的讨论可以总结为下面定理 6.

定理 6　设 π 是 $\mathrm{GL}_2(F)$ 的一个中心特征标为 η 的无限维不可约可容许表示, ψ 是 F 的阶为 $n(\psi)$ 的非平凡加法特征标, v_0 是 π 的在 Kirillov 模型 $\mathfrak{K}_\pi(\psi)$ 中的正规化新向量. 则 $L(\pi,U)$ 有两个极点的充要条件为: π 是由 $F^\times$ 的两个非分歧拟特征标 μ 和 ν 诱导出的主序列表示 $\pi(\mu,\nu)$, 这又等价于 π 是非分歧的. 此时

$$v_0 = \sum_{i=0}^{\infty} c_i \chi_0 U^{-n(\psi)+i},$$

其中 $c_0=1$, 且当 $i\geq 0$ 时, $\lambda c_i=c_{i+1}+q^{-1}\eta(\varpi)c_{i-1}$. 换句话说, v_0 是 Hecke 算子的一个特征值为 λ 的特征向量. 进一步

$$\begin{aligned}L(\pi,U)^{-1}&=(1-\mu(\varpi)U)(1-\nu(\varpi)U)\\&=1-\lambda q^{1/2}U+\eta(\varpi)U^2.\end{aligned}$$

其次, $L(\pi,U)$ 有一个极点的充要条件为: 或者 π 是主序列表示 $\pi(\mu,\nu)$, 其中 μ 和 ν 中有且只有一个是非分歧的; 或者 $\pi=\sigma(\mu,\nu)$, 其中 $\mu\nu^{-1}=|\ |^{\pm1}$ 且 μ 是非分歧的. 此时, 新向量 v_0 可表为

$$\sum_{i=0}^{\infty}b^i\chi_0U^{-n(\psi)+i},\quad L(\pi,U)^{-1}=1-bq^{1/2}U.$$

最后, $L(\pi,U)=1$ 的充要条件为: 新向量 $v_0=\chi_0U^{-n(\psi)}$. 不管上面哪种情况均有

$$\begin{aligned}\Phi(\mathrm{id},U,W_{v_0})&=\int_{F^\times}W_{v_0}\left(\begin{pmatrix}a&0\\0&1\end{pmatrix}\right)|a|^{-1/2}U^{\mathrm{ord}\,a}\mathrm{d}^\times a\\&=\int_{F^\times}v_0(a)|a|^{-1/2}U^{\mathrm{ord}\,a}d^\times a\\&=(q^{1/2}U)^{-n(\psi)}L(\pi,U).\end{aligned}$$

§3 F 是 Archimedes 局部域时 $\mathrm{GL}_2(F)$ 的表示

在这一节里, G 代表群 $\mathrm{GL}_2(\mathbf{R})$ 或 $\mathrm{GL}_2(\mathbf{C})$, 并将它视为 $\mathbf{R}$ 上的代数群; H 是一个可分的 Hilbert 空间; $\mathrm{GL}(H)$ 是 H 上可逆有界线性算子群. G 在 H 上的**表示** (π,H) 是一个同态映射

$$\pi:G\longrightarrow\mathrm{GL}(H),$$

且使得由 $(g,v)\longmapsto\pi(g)v$ 给出的映射 $G\times H\longrightarrow H$ 是连续的. 设 K 是 G 的标准最大紧子群. 内积

$$\langle v,v'\rangle=\int_K\langle\pi(k)v,\pi(k)v'\rangle_H\mathrm{d}\,k$$

是由 H 上原有的内积 $\langle\ ,\ \rangle_H$ 在 K 上平均而得到的，它在 H 上诱导出一个同 H 原有拓扑相同的拓扑. 这样我们可以假定 π 在 K 上的限制 $\pi|_K$ 是酉表示. 利用酉表示理论知道 K 的不可约表示都是有限维的. 记 K 的不可约酉表示等价类集为 $\widehat{K}$. 对 $\widehat{K}$ 中的任意等价类 γ, 设 H_γ 是 H 的 γ-同型 (isotypic) 子空间，即 H_γ 是 H 的一些子空间的直和，在每个子空间上，$\pi(K)$ 的作用同构于 γ. 若对任意的 $\gamma \in \widehat{K}$ (H_γ) 是有限维的，则称 (π, H) 是**可容许的**.

给定一个可容许表示 (π, H), 以 H_0 表 $H_\gamma(\gamma \in \widehat{K})$ 的代数和，即

$$H_0 = \{v \in H : v \text{ 生成的 } \pi(K) \text{ 不变子空间是有限维的}\}.$$

用 $\mathfrak{g}$ 表示 Lie 群 G 的 Lie 代数. 由 Harish-Chandra 的一个定理知，G 的一个可容许表示 (π, H) 导出 H_0 上 $\mathfrak{g}$ 的一个作用 π:

$$\pi(X)v = \frac{\mathrm{d}}{\mathrm{d}t}(\pi(\exp(tX))v)|_{t=0}, \quad X \in \mathfrak{g}, \quad v \in H_0.$$

$\pi(X)v$ 仍在 H_0 中，并且该作用满足：对任意的 $k \in K$, $X, Y \in \mathfrak{g}$ 和 $v \in H_0$,

(I) $\pi(k)\pi(X)v = \pi(\mathrm{Ad}(k)X)\pi(k)v$, 这里 Ad 是伴随表示;

(II) 在 H_0 上有 Lie 括号关系

$$\pi[X,Y] = \pi(X)\pi(Y) - \pi(Y)\pi(X) = [\pi(X), \pi(Y)].$$

这就导出了 $(\mathfrak{g}, K)$ 模的定义：如果复向量空间 V 满足条件

(1) V 是 $\mathfrak{g}$ 模，即存在线性映射

$$\mathfrak{g} \bigotimes V \longrightarrow V,$$

$$X \bigotimes v \longmapsto X \cdot v,$$

它满足关系：对任意的 $X, Y \in \mathfrak{g}$, $v \in V$, 有

$$[X,Y] \cdot v = X \cdot Yv - Y \cdot Xv;$$

(2) V 是 K 模，即存在映射 $K\times V\longrightarrow V$, 它在 V 上线性，且对任意的 $k_1,k_2\in K$, $v\in V$, 有

$$1\cdot v=v,\quad k_1\cdot(k_2\cdot v)=(k_1k_2)\cdot v;$$

(3) 对任意的 $v\in V$, 由 v 生成的 K 不变子空间是有限维的. 并且，若 W 是 V 的一个 K 不变子空间，它可分解成不可约的 K 不变子空间的直和，映射 $K\times W\longrightarrow W$ 是连续的，从而是实解析的；

(4) 若 X 在 K 的 Lie 代数中， $v\in V$, 则

$$X\cdot v=\frac{\mathrm{d}}{\mathrm{d}t}\exp(tX\cdot v)|_{t=0};$$

(5) 对 $k\in K$, $X\in\mathfrak{g}$, $v\in V$, 有

$$k\cdot X\cdot v=(\mathrm{Ad}(k)X)\cdot(k\cdot v).$$

则我们称 V 是一个 $(\mathfrak{g},K)$ **模**. 若对于任意的 $\gamma\in K$, V 的 γ-同型子空间是有限维的，则称该 $(\mathfrak{g},K)$ 模 V 是**可容许的**. 如果 V 中只有 $\{0\}$ 和 V 是 $\mathfrak{g}$ 和 K 的不变子空间，则称 $(\mathfrak{g},K)$ 模 V 是**不可约的**.

定理 7 (Harish-Chandra) (1) 设 (π,H) 是 G 的可容许表示 (于是 H_0 为可容许 $(\mathfrak{g},K)$ 模), 则 (π,H) 不可约的充要条件是 H_0 为一个不可约 $(\mathfrak{g},K)$ 模；

(2) 设 $(\pi_i,H_i)(i=1,2)$ 是 G 的两个可容许酉表示，则 π_i, π_2 是酉等价的充要条件是 $(\mathfrak{g},K)$ 模 $H_{1,0}$ 和 $H_{2,0}$ 同构；

(3) 设 V 是可容许 $(\mathfrak{g},K)$ 模，则存在 G 的一个可容许酉表示 (π,H) 使得 $V=H_0$ 的充要条件是 V 是酉的.

由此看出，确定 G 的可容许不可约酉表示的所有等价类等同于寻找不可约 $(\mathfrak{g},K)$ 模的同构类. 下面 Casselman 的结果是说，如果我们去掉“酉 ”这个限制，也有同样的结论.

定理 8 (Casselman) 设 V 是一个可容许不可约 $(\mathfrak{g},K)$ 模，则存在 G 的可容许不可约表示 (π,H), 使得 V 同构于 H_0.

上面的结论对于 G 是一个实约化 Lie 群同样也是成立的. 这方面的内容请读者参阅参考文献 [36]. 于是, 对 G 之表示的研究就转化为对 $(\mathfrak{g}, K)$ 模的研究. 此外, 对 G 之 Hecke 代数 $\mathcal{H}$ 的表示的研究与研究 $\mathfrak{g}$ 的通用包络代数 $\mathcal{U}(\mathfrak{g})$ 的表示等同. 今后为了方便, 有时我们均混称它们为 G 的表示.

回到 $G = \mathrm{GL}_2(\mathbf{R})$ 或 $\mathrm{GL}_2(\mathbf{C})$ 的情况. 下面, 一提到 G 表示均指 G 的可容许不可约表示. 我们概述一下有关 G 之表示的主要结果. 读者将会看到, 至多稍加变动, 上节的主要结论在这里都是成立的.

我们知道, $\mathbf{R}^\times$ 的拟特征标 μ 可以写成

$$\mu(t) = |t|_{\mathbf{R}}^r (\operatorname{sgn} t)^m, \quad r \in \mathbf{C},\ m = 0 \text{ 或 } 1$$

的形式; $\mathbf{C}$ 的拟特征标则有形式

$$\varpi(z) = |z|_{\mathbf{C}}^r z^m \bar{z}^n, \quad r \in \mathbf{C},\ m, n \in \mathbf{Z}_{\geq 0},\ \text{且 } mn = 0$$

(注意在这里 $|z|_{\mathbf{C}} = z\bar{z}$). 给出 $\mathbf{R}^\times$ 的两个拟特征标 μ 和 ν, 若

$$\mu\nu^{-1}(t) \neq |t|_{\mathbf{R}}^p \operatorname{sgn} t,$$

其中 $p \in \mathbf{Z}\backslash\{0\}$, 则它们可诱导出 $\mathrm{GL}_2(\mathbf{R})$ 的一个不可约表示 $\pi = \pi(\mu, \nu)$; 若存在非 0 整数 p, 使得

$$\mu\nu^{-1}(t) = |t|_{\mathbf{R}}^p \operatorname{sgn} t,$$

则诱导出的表示就不是不可约的, 不过它包含了唯一一个无限维不可约表示 $\sigma(\mu, \nu)$; 利用 Weil 表示的方法, 对 $\mathbf{C}$ 的每个拟特征标 ω, 我们总可找到 $\mathrm{GL}_2(\mathbf{R})$ 的一个无限维表示 $\pi(\omega)$, 可以证明 $\pi(\omega)$ 一定是 $\sigma(\mu, \nu)$ 型的表示. 从而, $\mathrm{GL}_2(\mathbf{R})$ 的无限维表示只有 $\pi(\mu, \nu)$ 和 $\sigma(\mu, \nu)$ 这两种.

设 $\psi(x) = \mathrm{e}^{2\pi i u x}$ 是 $\mathbf{R}$ 的一个非平凡加法特征标. 由从 Tate 的博士论文 [32] 发展出的 GL_1 之表示的局部理论知道, 对 $\mathbf{R}^\times$ 的拟特征标

$$\mu(t) = |t|_{\mathbf{R}}^r (\operatorname{sgn} t)^m,$$

它结合了一个 L 因子

$$L(\mu,s)=\pi^{-(s+r+m)/2}\Gamma\left(\frac{s+r+m}{2}\right)$$

和一个 ε 因子

$$\varepsilon(\mu,\psi,s)=(\mathrm{i}\ \mathrm{sgn}\, u)^m|u|_{\mathbf{R}}^{s+r-\frac{1}{2}}.$$

而对 $\mathbf{C}^\times$ 的拟特征标 $\omega(z)=|z|_{\mathbf{C}}^r z^m\bar{z}^n$, 其结合的 L 因子和 ε 因子分别为

$$L(\omega,s)=2(2\pi)^{-(s+r+m+n)}\Gamma(s+r+m+n),$$

$$\varepsilon(\omega,\phi,s)=\mathrm{i}^{m+n}\omega(w)|w|_{\mathbf{C}}^{s-\frac{1}{2}},$$

其中 $\phi(z)=\mathrm{e}^{4\pi\mathrm{i}\mathrm{Re}(wz)}=\mathrm{e}^{2\pi\mathrm{i}\,\mathrm{Tr}(wz)}$. 现在定义 $\mathrm{GL}_2(\mathbf{R})$ 的 L 因子和 ε 因子分别为

$$L(\pi,s)=\begin{cases}L(\mu,s)L(\nu,s), & \pi=\pi(\mu,\nu),\\ L(\omega,s), & \pi=\pi(\omega),\end{cases}$$

$$\varepsilon(\pi,\psi,s)=\begin{cases}\varepsilon(\mu,\psi,s)\varepsilon(\nu,\psi,s), & \pi=\pi(\mu,\nu),\\ (\mathrm{i}\,\mathrm{sgn}\, u)\varepsilon(\omega,\psi\circ\mathrm{Tr}_{\mathbf{C}/\mathbf{R}},s), & \pi=\pi(\omega),\end{cases}$$

其中 $\psi(x)=\mathrm{e}^{2\pi\mathrm{i}ux}$, $u\in\mathbf{R}^\times$. 在 $\pi(\omega)=\pi(\mu,\nu)$ 这种情况, 两种定义是一致的, 这可以从 Γ 函数所满足的补元公式得到.

Jacquet 和 Langlands 证明了 $\mathrm{GL}_2(\mathbf{R})$ 的一个无限维表示 π 的等价类可以被函数

$$\gamma_\pi(\chi,\psi,s)=\frac{L(\tilde{\pi}\otimes\chi^{-1},1-s)}{L(\pi\otimes\chi,s)}\varepsilon(\pi\otimes\chi,\psi,s)$$

所确定, 其中 χ 是 $\mathbf{R}^\times$ 的一个拟特征标. 更进一步, 同样可以建立 Whittaker 模型和局部函数方程. 准确地说, 就是

定理 9 (Jacquet-Langlands[17]) 设 π 是 $\mathrm{GL}_2(\mathbf{R})$ 的一个无限维可容许不可约表示, ψ 是 $\mathbf{R}$ 的一个非平凡加法特征标, η 为 π 的中心特征标. 则

(1) 唯一存在 $\mathrm{GL}_2(\mathbf{R})$ 的 Whittaker 模型 $\mathfrak{W}_\pi(\psi)$, 它所包含的 Whittaker 函数 W 具有下列性质:

(a) 对任意的 $x \in \mathbf{R}$, $g \in \mathrm{GL}_2(\mathbf{R})$,

$$W\left(\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} g\right) = \psi(x)W(g);$$

(b) 存在 $N > 0$, 使得当 $|t|_{\mathbf{R}}$ 趋于 ∞ 时，有

$$W\left(\begin{pmatrix} t & 0 \\ 0 & 1 \end{pmatrix} g\right) = O(|t|_{\mathbf{R}}^N);$$

(c) W 是个连续函数；此外，$\mathfrak{W}_\pi(\psi)$ 上通过将 K 的作用定义为右平移，$X \in \mathfrak{g}$ 的作用定义为

$$X \cdot W(g) = \frac{\mathrm{d}}{\mathrm{d}t} W(g \exp(tX))|_{t=0}$$

而得到的 $(\mathfrak{g}, K)$ 模同构于由 π 得到的 $(\mathfrak{g}, K)$ 模.

(2) 对 $W \in \mathfrak{W}_\pi(\psi)$, 定义

$$\varPhi(g, s, W) = \int_{\mathbf{R}^\times} W\left(\begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix} g\right) |a|^{s-\frac{1}{2}} \mathrm{d}^\times a,$$

$$\widetilde{\varPhi}(g, s, W) = \int_{\mathbf{R}^\times} W\left(\begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix} g\right) \eta^{-1}(a)|a|^{s-\frac{1}{2}} \mathrm{d}^\times a.$$

则，当 $\mathrm{Re}\, s$ 充分大时，$\varPhi$ 和 $\widetilde{\varPhi}$ 都是绝对收敛的. 进一步，函数 $\varPhi(g, s, W)/L(\pi, s)$ 和函数 $\widetilde{\varPhi}(g, s, W)/L(\widetilde{\pi}, s)$ 都可以解析开拓为整个 s 平面上的亚纯函数，且满足函数方程：对任意的 $g \in \mathrm{GL}_2(\mathbf{R})$, $W \in \mathfrak{W}_\pi(\psi)$,

$$\frac{\widetilde{\varPhi}(wg, 1-s, W)}{L(\widetilde{\pi}, 1-s)} = \varepsilon(\pi, \psi, s) \frac{\varPhi(g, s, W)}{L(\pi, s)}.$$

此外，固定 W, 当 g 在一个紧子集中变化，s 在除去以 $L(\pi, s)$ 的极点为圆心的小圆盘后的区域里变化时，$\varPhi(g, s, W)$ 是有界的. 最后，在 $\mathfrak{W}_\pi(\psi)$ 中可以找到函数 W, 使得函数 $\varPhi(\mathrm{id}, s, W)$ 等于 $L(\pi, s)$ 乘上一个 s 的指数函数.

$GL_2(\mathbf{C})$ 的表示理论与 $GL_2(\mathbf{R})$ 的类似，并且还要简单一些. 对 $GL_2(\mathbf{C})$ 任意的无限维表示 π, 都能找到 $\mathbf{C}^\times$ 的两个拟特征标 μ 和 ν, 使得 $\pi = \pi(\mu, \nu)$. 它的 L 因子和 ε 因子分别为

$$L(\pi, s) = L(\mu, s)L(\nu, s) \quad 和 \quad \varepsilon(\pi, \psi, s) = \varepsilon(\mu, \psi, s)\varepsilon(\nu, \psi, s).$$

在定理 9 中把 $\mathbf{R}$ 换成 $\mathbf{C}$, 结论仍然成立.

§4 GL_2 的自守表示

设 F 是整体域. 以 $GL_2(A_f)$ 记 $GL_2(A_F)$ 中的有限阿代尔点构成的群，即它是 $\{GL_2(F_v)\}$ 关于 $\{GL_2(\mathcal{O}_v)\}$ 的限制直积，其中 v 过 F 的所有有限位. 用 $GL_2(A_\infty)$ 表示积

$$\prod_\sigma GL_2(F_\sigma),$$

其中 σ 过 F 的所有 Archimedes 位. 显然，当 F 是函数域时，$GL_2(A_\infty)$ 是平凡的. 设 $\mathfrak{g}_\sigma$ 为 $GL_2(F_\sigma)$ 的 Lie 代数，那么 $GL_2(A_\infty)$ 的 Lie 代数 $\mathfrak{g}_\infty$ 就是 $\prod\limits_\sigma \mathfrak{g}_\sigma$. 设 K_σ 是 $GL_2(F_\sigma)$ 的标准最大紧子群，命

$$K_\infty = \prod_\sigma K_\sigma.$$

对 $GL_2(A_f)$ 的一个表示，如果它的表示空间中的任意向量都在 $GL_2(A_f)$ 的某个紧开子群作用下不变，则我们称它是**光滑的**. V 是 $GL_2(A_F)$ 的一个表示意味着 V 同时是一个 $(\mathfrak{g}_\infty, K_\infty)$ 模和一个 $GL_2(A_f)$ 模，并且

(1) $GL_2(A_f)$ 的作用与 $\mathfrak{g}_\infty$ 和 K_∞ 的作用交换;

(2) 设

$$K_f = \prod_v GL_2(\mathcal{O}_v),$$

v 跑遍 F 的有限位. 对 $K = K_\infty K_f$ 的每个连续不可约表示类 γ, V 所含的 γ-同型子空间 V_γ 是有限维的.

一个可容许 $(\mathfrak{g}_\infty, K_\infty)$ 模总可以分解为不可约可容许 $(\mathfrak{g}_\sigma, K_\sigma)$ 模的张量积, 这里 σ 跑遍 F 的 Archimedes 位. 不过, 对 $\mathrm{GL}_2(A_f)$ 的光滑表示 V_f 尚需进一步的解释.

从 V_f 的光滑性可知, V_f 中的任意向量对几乎所有的位 v 均在 $\mathrm{GL}_2(\mathcal{O}_v)$ 的作用下不变. 由此导致下面的构造: 在 F 的每个有限位 v 处, 假设在空间 V_v 上给出了 $\mathrm{GL}_2(F_v)$ 的表示 π_v, 使得对几乎所有的 v, V_v 中由 $\mathrm{GL}_2(\mathcal{O}_v)$ 不变向量组成的空间不为零. 以 Σ_0 记额外的有限位集, 换言之, Σ_0 由不含非零 $\mathrm{GL}_2(\mathcal{O}_v)$ 不变向量的有限位 v 组成. 对 F 的任意不含在 Σ_0 中的位 v, 取定 V_v 中一个在 $\mathrm{GL}_2(\mathcal{O}_v)$ 作用下不变的非零向量 v_v. 对一个由有限个 F 的有限位组成的集合 S, 且 $S \supset \Sigma_0$, 命

$$V_S = \bigotimes_{v \in S} V_v.$$

设 S 和 S' 是两个这样的集, 且 $S \subset S'$, 利用把 x 与 $x \bigotimes_{v \in S'-S} v_v$ 等同, 可将 V_S 嵌入到 $V_{S'}$ 中去. 当 S 跑遍所有包含 Σ_0 的 F 的有限位的有限集时, 正向极限 $\lim\limits_{\vec{S}} V_S$ 被称为 $\{V_v\}$ 关于 $\{v_v\}$ 的限制张量积, 记作 $\bigotimes'_{\{v_v\}} V_v$. 它是由向量 $\bigotimes_v x_v$ 生成的, 其中 $x_v \in V_v$, 并且对几乎所有的 v 而言, 都有 $x_v = v_v$. 群 $\mathrm{GL}_2(A_f)$ 通过 π_v 以明显方式作用于 $\bigotimes'_{\{v_v\}} V_v$ 上. 尽管空间 $\bigotimes'_{\{v_v\}} V_v$ 依赖于 v_v 的选取, 但如果我们改变基向量 v_v 的选取, 所得到的 $\mathrm{GL}_2(A_f)$ 模仍是同构的. 我们称此表示为 $\{\pi_v\}$ 的限制张量积 $\bigotimes'_v \pi_v$. 可以证明, 如果每个 π_v 是可容许不可约的, 则 $\bigotimes'_v \pi_v$ 是光滑不可约的. 事实上, 它也是可容许的, 即对 K_f 的每个紧开子群 H, 由 H 不变向量组成的空间是有限维的. 因此, 对 Archimedes 位 σ, 给出一个可容许不可约 $(\mathfrak{g}_\sigma, K_\sigma)$ 模 π_σ; 对有限位 v, 给出 $\mathrm{GL}_2(F_v)$ 模 π_v, 限制张量积

$$\pi = \bigotimes_\sigma \pi_\sigma \bigotimes \bigotimes'_{v\text{有限位}} \pi_v = \bigotimes'_v \pi_v$$

是 $\mathrm{GL}_2(A_F)$ 的可容许不可约表示. 反过来, $\mathrm{GL}_2(A_F)$ 的任意可容

许不可约表示均可以通过这种方式得到.

仍旧用 $\mathcal{A}(\mathrm{GL}_2(A_F),\eta)$ 表示 $\mathrm{GL}_2(A_F)$ 上中心特征为 η 的自守函数空间. $\mathrm{GL}_2(A_F)$ 在 $\mathcal{A}(\mathrm{GL}_2(A_F),\eta)$ 上的正则表示意味着 $K_\infty \mathrm{GL}_2(A_f)$ 以右平移的方式作用, $\mathfrak{g}_\infty$ 则以微分算子出现, 即, 对 $X\in\mathfrak{g}_\infty$, 它映一个自守形式 f 为

$$X\cdot f(g)=\frac{\mathrm{d}}{\mathrm{d}t}f(g\exp(tX))|_{t=0}.$$

对 $\mathrm{GL}_2(A_F)$ 的可容许不可约表示 π, 如果存在 $\mathcal{A}(\mathrm{GL}_2(A_F),\eta)$ 的两个 $\mathrm{GL}_2(A_F)$ 不变子空间 V 和 W, $V\subset W$, 使得 π 同构于在 W/V 上诱导出的作用, 则我们称它是**自守表示**, 并说表示 π 是此正则表示的一个**组成份子**. 当 $V=\{0\}$ 时, π 称作**子表示**; 但在 $V\neq\{0\}$ 时, π 称作**子商**. 若 V 和 W 包含在尖点形式空间 $\mathcal{A}^0(\mathrm{GL}_2(A_F),\eta)$ 中, 则 π 称为 $\mathrm{GL}_2(A_F)$ 的**尖点表示**.

下面, 我们将概述一下有关 GL_2 的自守表示的主要结果. 读者可以参阅 Jacquet 和 Langlands 的著作 [17] 以及参考文献 [21], [3], [10] 和 [13].

定理 10(Jacquet-Langlands[17, 第 340 页]) 设

$$\pi=\bigotimes_v{}' \pi_v$$

是 $\mathrm{GL}_2(A_F)$ 的一个可容许不可约自守表示, 如果它不是尖点表示, 则存在 $I_F/F^\times$ 的两个伊代尔类特征标 μ 和 ν, 使得在每个有限位 v 处, 表示 π_v 是诱导表示 $\rho(\mu,\nu)$ 的一个组成份子.

这个定理实际上是: “给定参数的模形式空间均是 Eisenstein 空间和尖点形式空间的直和” 这个结论的表示论的模拟表述.

Jacquet 和 Langlands 又证明了尖点形式空间 $\mathcal{A}^0(\mathrm{GL}_2(A_F),\eta)$ 可以分解为不可约尖点表示的直和, 且每个不可约尖点表示出现的重数是有限的. 换句话说, 尖点表示是子表示. 我们主要是研究尖点表示. 设 ϕ 是在一个尖点表示

$$\pi=\bigotimes_v{}' \pi_v$$

的表示空间中的尖点形式. 若 F 是一个函数域, 记 X 为使 ϕ 在

$$\begin{pmatrix} 1 & y \\ 0 & 1 \end{pmatrix}$$

的右作用下不变的元 $y \in A_F$ 的集合. 利用第四章中的推论 4, 存在常数 $c_1 > 0$, 使得对任意的 $a \in I_F$ 且 $|a| > c_1$, 有 $A_F = F + aX$. 这就导出, 对任意的 $z = ay$, 其中 $y \in X$, 有

$$\begin{aligned} \phi\left(\begin{pmatrix} 1 & z \\ 0 & 1 \end{pmatrix}\begin{pmatrix} a & x \\ 0 & 1 \end{pmatrix}\right) &= \phi\left(\begin{pmatrix} a & x \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & y \\ 0 & 1 \end{pmatrix}\right) \\ &= \phi\left(\begin{pmatrix} a & x \\ 0 & 1 \end{pmatrix}\right). \end{aligned}$$

由于上式对 $z \in F$ 也成立, 进而公式对所有的 $z \in A_F$ 成立. 因此, 对任意的 $|a| > c_1$ 和 $x \in A_F$ 有

$$\begin{aligned} \phi\left(\begin{pmatrix} a & x \\ 0 & 1 \end{pmatrix}\right) = & \frac{1}{\operatorname{meas}(A_F/F)} \\ & \times \int_{A_F/F} \phi\left(\begin{pmatrix} 1 & z \\ 0 & 1 \end{pmatrix}\begin{pmatrix} a & x \\ 0 & 1 \end{pmatrix}\right) dz = 0. \end{aligned}$$

这说明 ϕ 的支集是紧的且位于 $\mathrm{GL}_2(F)\mathcal{Z}(A_F)\backslash \mathrm{GL}_2(A_F)$ 中. 又由关系

$$\phi\left(\begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix}\right) = \phi\left(w\begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix}\right) = \eta^{-1}(a)\phi\left(\begin{pmatrix} a^{-1} & 0 \\ 0 & 1 \end{pmatrix} w\right)$$

和 ϕ 关于 w 的右平移也是尖点形式可知, 存在 $c_2 > 0$, 使得当 $|a^{-1}| > c_2$, 即 $|a| < c_2^{-1}$ 时,

$$\phi\left(\begin{pmatrix} a^{-1} & 0 \\ 0 & 1 \end{pmatrix} w\right) = 0.$$

于是作为 $a \in I_F$ 的函数,

$$\phi\left(\begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix}\right)$$

的支集是紧的且位于 $I_F/F^\times$ 中; 若 F 是数域, 对应的结果是

增长条件 对任意实数 M_1, 存在实数 M_2, 使得对所有的 $a \in I_F$, 有

$$\left|\phi\left(\begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix}\right)\right| \le M_2|a|^{M_1}.$$

作为 ϕ 之增长条件的推论, 每个 π_v 是无限维的.

设 $\pi = \bigotimes_v' \pi_v$ 是 $\mathrm{GL}_2(A_F)$ 的不可约自守表示, 且每个分支 π_v 是无限维的. 取在 F 上平凡的 A_F 的非平凡特征标

$$\psi = \prod_v \psi_v.$$

利用 §2 和 §3 的讨论可知, 每个 π_v 都结合有一个 Whittaker 模型 $\mathfrak{W}_{\pi_v}(\psi_v)$. 当 π_v 非分歧时, 在位 v 处, 取正规化的新向量 W_v. 命 $\mathfrak{W}_\pi(\psi)$ 是 $\{\mathfrak{W}_{\pi_v}(\psi_v)\}$ 关于 $\{W_v\}$ 的限制张量积, 则每个 $\mathfrak{W}_\pi(\psi)$ 中的函数 W 都是 $\mathrm{GL}_2(A_F)$ 上满足

$$W\left(\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} g\right) = \psi(x)W(g), \quad x \in A_F,\ g \in \mathrm{GL}_2(A_F)$$

的连续函数. 进而, $\mathrm{GL}_2(A_F)$ 在 $\mathfrak{W}_\pi(\psi)$ 上的作用同构于 π. 可以证明 $\mathfrak{W}_\pi(\psi)$ 这样的空间是唯一的. 此外, 如果 π 有分支 π_v 是有限维的, 则这样的空间不存在.

设 $\pi = \bigotimes_v' \pi_v$ 是 $\mathrm{GL}_2(A_F)$ 的不可约自守表示, 且每个分支 π_v 是无限维的. 按照 §2 和 §3 的方法已有了局部 L 因子和 ε 因子. 现把它们合在一起, 定义整体 L 因子和 ε 因子. 设

$$L(\pi, s) = \prod_v L(\pi_v, s), \quad L(\widetilde{\pi}, s) = \prod_v L(\widetilde{\pi}_v, s),$$

其中, 在非 Archimedes 位 v 处, $L(\pi_v, s)$ 和 $L(\widetilde{\pi}_v, s)$ 分别表示 $L(\pi_v, (\mathrm{N}v)^{-s})$ 和 $L(\widetilde{\pi}_v, (\mathrm{N}v)^{-s})$. 命

$$\varepsilon(\pi, \psi, s) = \prod_v \varepsilon(\pi_v, \psi_v, s),$$

其中, 在非 Archimedes 位 v 处, $\varepsilon(\pi_v, \psi_v, s)$ 表示函数 $\varepsilon(\pi_v, \psi_v, (\mathrm{N}v)^{-s})$. 由于 π 的中心特征标 η 是伊代尔类特征标, 再联系局部

ε 因子与加法特征标 ψ 的关系，我们发现只要 ψ 在 F 上平凡及在 A_F 上非平凡， $\varepsilon(\pi,\psi,s)$ 就不依赖于 ψ 的选取. 于是我们把它记为 $\varepsilon(\pi,s)$. L 因子的解析性质可概述为

定理 11(整体函数方程[17]) 设 $\pi=\bigotimes_v'\pi_v$ 是 $\mathrm{GL}_2(A_F)$ 一个不可约可容许自守表示. 则上面定义的 $L(\pi,s)$ 和 $L(\widetilde{\pi},s)$ 作为无穷乘积在右半平面上是绝对收敛的，并且可以解析开拓到整个 s 平面上，成为一个亚纯函数. 如果 π 是尖点表示，则它们更是整函数. 当 F 是数域时，它们有有限多个极点，并且在任意一个有限宽的竖条区域里的 ∞ 处有界. 当 F 是函数域时，设其常数域的势为 q, 则它们均是 q^{-s} 的有理函数. 此外，无论 F 是数域还是函数域，它们满足函数方程

$$L(\pi,s)=\varepsilon(\pi,s)L(\widetilde{\pi},1-s).$$

我们首先解释 π 不是尖点表示时的情况. 利用定理 10, 存在 $I_F/F^\times$ 的两个拟特征标 μ 和 ν, 使得 π_v 是 $\rho(\mu_v,\nu_v)$ 的一个组成份子. 由于对几乎所有的位 v, π_v 是非分歧的，所以对几乎所有 v,

$$\pi_v=\pi(\mu_v,\nu_v).$$

先假定对所有的位 v, $\pi_v=\pi(\mu_v,\nu_v)$, 则

$$L(\pi,s)=L(\mu,s)L(\nu,s),\quad L(\pi,s)=L(\mu^{-1},s)L(\nu^{-1},s).$$

从而解析性质可以从伊代尔类特征标的 L-函数的解析性质得到. 当 F 是函数域时，这已在第五章里证明了；当 F 是数域时，则可参阅 Tate 的博士论文 [32]. 再考虑存在有限多个位 v, 使得

$$\pi_v=\sigma(\mu_v,\nu_v)$$

的情况. 此时， $L(\pi,s)$ 与 $L(\mu,s)L(\nu,s)$ 相差有限多个因子，并且 $L(\pi,s)L(\mu,s)^{-1}L(\nu,s)^{-1}$ 在 F 是数域时它是全纯的，且在有限宽的竖条区域里有界；而当 F 是函数域时，它则是 q^{-s} 的一个多项式. 因此，利用局部 ε 因子的定义得到

$$\frac{L(\pi,s)}{L(\mu,s)L(\nu,s)}=\frac{\varepsilon(\pi,s)}{\varepsilon(\mu,s)\varepsilon(\nu,s)}\frac{L(\widetilde{\pi},1-s)}{L(\mu^{-1},1-s)L(\nu^{-1},1-s)}.$$

因此在这种情况下定理依然成立.

接下来研究 π 是作用在 $\mathcal{A}^0(\mathrm{GL}_2(A_F),\eta)$ 中尖点表示上的情况. 设 ϕ 是一个尖点形式, 从 §1 可知, 它的 Fourier 变换

$$W(g)=\int_{F\backslash A_F}\phi\left(\begin{pmatrix}1 & x\\ 0 & 1\end{pmatrix}g\right)\psi(-x)\mathrm{d}x,\quad g\in\mathrm{GL}_2(A_F)$$

是空间 $\mathfrak{W}_\pi(\psi)$ 中的 Whittaker 函数, 并且

$$\phi(g)=\sum_{\alpha\in F^\times}W\left(\begin{pmatrix}\alpha & 0\\ 0 & 1\end{pmatrix}g\right),\quad g\in\mathrm{GL}_2(A_F).$$

因此我们将在 Whittaker 函数空间上工作. 在有限位 v 处, 命 W_v 是 $\mathfrak{W}_{\pi_v}(\psi)$ 中的正规化新形式, 于是

$$\begin{aligned}&\int_{F_v^\times}W_v\left(\begin{pmatrix}a_v & 0\\ 0 & 1\end{pmatrix}\right)|a_v|_v^{s-\frac{1}{2}}\mathrm{d}^\times a\\ &\qquad=(\mathrm{N}v)^{-n(\psi_v)(\frac{1}{2}-s)}L(\pi_v,(\mathrm{N}v)^{-s}),\end{aligned}$$

其中 $n(\psi)$ 是 ψ 的阶; 在 Archimedes 位 v 处命 W_v 是 $\mathfrak{W}_{\pi_v}(\psi_v)$ 中的函数, 使得

$$\begin{aligned}&\int_{F_v^\times}W_v\left(\begin{pmatrix}a_v & 0\\ 0 & 1\end{pmatrix}\right)|a_v|_v^{s-\frac{1}{2}}\mathrm{d}^\times a\\ &\qquad=(s\text{ 的指数函数})L(\pi_v,(\mathrm{N}v)^{-s}).\end{aligned}$$

令 $W=\bigotimes_v W_v$, 显然它在 $\mathfrak{W}_\pi(\psi)$ 中. 命

$$\phi(g)=\sum_{\alpha\in F^\times}W\left(\begin{pmatrix}\alpha & 0\\ 0 & 1\end{pmatrix}g\right),\quad g\in\mathrm{GL}_2(A_F),$$

它是一个尖点形式. 以 $\mathrm{d}^\times a$ 表示 I_F 的由 $\prod_v\mathrm{d}^\times a_v$ 导出的 Haar 测度. 考虑积分

$$\begin{aligned}\varPhi(\mathrm{id},s,W)&=\int_{F^\times\backslash I_F}\phi\left(\begin{pmatrix}a & 0\\ 0 & 1\end{pmatrix}\right)|a|^{s-\frac{1}{2}}\mathrm{d}^\times a\\ &=\int_{F^\times\backslash I_F}\sum_{\alpha\in F^\times}W\left(\begin{pmatrix}\alpha & 0\\ 0 & 1\end{pmatrix}\begin{pmatrix}a & 0\\ 0 & 1\end{pmatrix}\right)|a|^{s-\frac{1}{2}}\mathrm{d}^\times a\end{aligned}$$

$$
\begin{aligned}
&= \int_{I_F} W\left(\begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix}\right) |a|^{s-\frac{1}{2}} \mathrm{d}^\times a \\
&= \prod_v \int_{F_v^\times} W\left(\begin{pmatrix} a_v & 0 \\ 0 & 1 \end{pmatrix}\right) |a_v|^{s-\frac{1}{2}} \mathrm{d}^\times a \\
&= \prod_v \Phi(\mathrm{id}, s, W) = (s \text{ 的指数函数}) L(\pi, s).
\end{aligned}
$$

此处最后一个等号成立是因为对几乎所有的 v, $n(\psi_v) = 0$. ϕ 满足的增长条件不仅表明用无穷乘积定义的函数 $L(\pi, s)$ 在 $\mathrm{Re}\, s \gg 0$ 时绝对收敛, 而且说明 ϕ 在 $F^\times \setminus I_F$ 上的积分在整个平面上定义了一个整函数, 当 F 是数域时, 它在有限宽竖条区域里有界; 当 F 是函数域时, 它则是 q^{-s} 的一个有限 Laurent 级数. 事实上, 当 F 是函数域时, 利用在 $\mathrm{Re}\, s \to \infty$ 时, $L(\pi, s) \to 1$ 这一结果可以断言 $L(\pi, s)$ 是 q^{-s} 的具有非 0 常数项的多项式. 此外函数 $L(\pi, s)$ 在 $\mathrm{Re}\, s \gg 0$ 时的绝对收敛性也可以由下面事实看出: 对几乎所有的位 v, 存在 F_v 的两个非分歧的拟特征标 μ_v 和 ν_v, 使得

$$
\pi_v = \pi(\mu_v, \nu_v),
$$

且满足

$$
\begin{aligned}
|\eta_v(\varpi_v)|^{1/2} (\mathrm{N}v)^{-1/2} &\le |\mu_v(\varpi_v)|, \\
|\nu_v(\varpi_v)| &\le |\eta_v(\varpi_v)|^{1/2} (\mathrm{N}v)^{1/2}.
\end{aligned}
$$

类似地, 对 π 的逆步表示 $\widetilde{\pi}$, 取

$$
w = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix},
$$

积分

$$
\begin{aligned}
\widetilde{\Phi}(w, s, W) &= \int_{F^\times \setminus I_F} \phi\left(\begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix} w\right) \eta(a)^{-1} |a|^{s-\frac{1}{2}} \mathrm{d}^\times a \\
&= \prod_v \int_{F_v^\times} W_v\left(\begin{pmatrix} a_v & 0 \\ 0 & 1 \end{pmatrix} w_v\right) \eta_v(a_v)^{-1} |a_v|^{s-\frac{1}{2}} \mathrm{d}^\times a_v
\end{aligned}
$$

$$= \prod_v \widetilde{\Phi}_v(w_v, s, W_v) = (s \text{ 的指数函数}) L(\widetilde{\pi}, s)$$

给出 $L(\widetilde{\pi}, s)$ 的解析开拓. 为了得到它的函数方程, 需要结合在 §2 和 §3 讨论的局部理论以及 ϕ 的自守性. 简要地讲, 由

$$\phi\left(\begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix}\right) = \phi\left(w\begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix}\right) = \phi\left(\begin{pmatrix} 1 & 0 \\ 0 & a \end{pmatrix} w\right)$$

$$= \eta(a)\phi\left(\begin{pmatrix} a^{-1} & 0 \\ 0 & 1 \end{pmatrix} w\right)$$

得 $\Phi(\mathrm{id}, s, W) = \widetilde{\Phi}(w, 1-s, W)$. 另一方面, 由定理 4 和定理 9, 对所有的位 v, 我们有

$$\frac{\widetilde{\Phi}_v(w, 1-s, W_v)}{L(\widetilde{\pi}_v, 1-s)} = \varepsilon(\pi_v, \psi_v, s)\frac{\Phi_v(\mathrm{id}, s, W_v)}{L(\pi_v, s)}.$$

过所有的位 v 对上面方程求积, 再结合

$$\prod_v \widetilde{\Phi}_v(w, 1-s, W_v) = \widetilde{\Phi}(w, 1-s, W)$$

和

$$\Phi(\mathrm{id}, s, W) = \prod_v \Phi_v(\mathrm{id}, s, W_v),$$

我们就得到了所求函数方程.

注 当 $K = \mathbf{Q}$ 时, 取 ψ 是 $A_{\mathbf{Q}}/\mathbf{Q}$ 的标准加法特征标, 使得对所有有限位 v, $n(\psi) = 0$. 存在正整数 N, 使得

$$\varepsilon(\pi, s) = \text{常数} \cdot N^{-s}.$$

我们称 N 是表示 π 的**前导子**. 当 π_∞ 是 $\mathrm{GL}_2(\mathbf{R})$ 的离散序列表示, 且 $r(\theta) \in K_\infty$ 的作用是乘以 $r(k\theta)$ 时, 如前由

$$W = \bigotimes\nolimits_v W_v$$

所得的函数 ϕ 是一个权 k, 水平 N, 特征标为 η 的新形式, 其中, 对有限位 v, W_v 是正规化的新向量. 记 ϕ 的规范化为 ϕ'. 按第七

章方式定义的 ϕ' 的 L-函数经过变量代换后恰好是 π 的 L-函数，即

$$L(\phi', s+(k-1)/2) = L(\pi, s).$$

反过来，给定一个正规化的尖点新形式 ϕ'，存在唯一的 $\mathrm{GL}_2(A_{\mathbf{Q}})$ 的尖点表示 π，使得

$$L(\pi, s) = L(\phi', s+(k-1)/2).$$

由第七章定义的 ϕ' 的提升都位于 π 对应的表示空间里.

同模形式论一样，我们有下面的反问题：在 F 的每个位 v 处，给出 $\mathrm{GL}_2(F_v)$ 的可容许不可约表示 π_v，其中对几乎所有的位 v，存在特征标 μ_v 和 ν_v，它们满足

$$(\mathrm{N}v)^{-c} \le |\mu_v(\varpi_v)|, \quad |\nu_v(\varpi_v)| \le (\mathrm{N}v)^c$$

(这里 c 是一个不依赖于 v 的常数)，使得 $\pi_v = \pi(\mu_v, \nu_v)$ 是非分歧的，它们的限制张量积 $\pi = \bigotimes_v' \pi_v$ 是 $\mathrm{GL}_2(A_F)$ 的一个可容许不可约表示 π，并且其 L-函数 $L(\pi, s)$ 在右半平面上绝对收敛. 那么 π 什么时候是一个自守表示呢？对 π 何时是尖点表示的研究是由 Jacquet 和 Langlands[17] 做出的，他们借助于 π 的 L-函数 $L(\pi, s)$ 以及它关于 $I_F/F^\times$ 的所有拟特征标的扭曲所得的 L-函数的解析性质对上述问题给予了回答.

定理 12(**GL_2的逆定理**)　如上定义的表示 π 是 $\mathrm{GL}_2(A_F)$ 的一个尖点表示的充分必要条件是，对 $I_F/F^\times$ 的任意特征标 χ，函数 $L(\pi \bigotimes \chi, s)$ 和 $L(\widetilde{\pi} \bigotimes \chi^{-1}, s)$ 在整个 s 平面上有全纯开拓，并满足函数方程

$$L(\pi \bigotimes \chi, s) = \varepsilon(\pi \bigotimes \chi, s) L(\widetilde{\pi} \bigotimes \chi^{-1}, 1-s),$$

以及，当 F 是数域时，这些 L-函数在任意有限宽的竖条区域上有界；当 F 是函数域时，这些 L-函数均为 q^{-s} 的多项式，这里 q 是 F 的常数域的势.

在此需要说明两点：第一，在证明充分性时仅需要用到对那些前导子整除 π 的前导子的特征标 χ，函数 $L(\pi\otimes\chi,s)$ 有所述的解析性质；第二，对于非尖点表示的自守表示也有类似的结论，有兴趣的读者可以参阅参考文献 [25].

最后需要指出的是 Jacquet 和 Langlands 事实上证明了下面的结论：

重数一定理 设 π 是出现于尖点形式空间 $\mathcal{A}^0(\mathrm{GL}_2(A_F),\eta)$ 的不可约尖点表示，则它在 $\mathcal{A}^0(\mathrm{GL}_2(A_F),\eta)$ 中出现的重数为 1.

实际上，我们有更强的结论：

强重数一定理 设

$$\pi_i=\bigotimes_v{}'\,\pi_{v,i}\quad(i=1,2)$$

是两个出现于 $\mathcal{A}^0(\mathrm{GL}_2(A_F),\eta)$ 的不可约尖点表示. 假定在几乎所有 F 的位 v 处，$\pi_{v,1}$ 和 $\pi_{v,2}$ 是同构的，则 $\pi_{v,1}$ 和 $\pi_{v,2}$ 对所有的位 v 都同构，进而 π_1 与 π_2 同构.

Shalika[30] 证明这个定理对 GL_n 也是成立的. 不过在 $n\geq 3$ 时，要求 $\pi_{v,1}$ 和 $\pi_{v,2}$ 在所有的 Archimedes 位 v 处都是同构的. 读者可以参阅 Piatetski-Shapiro 的文章 [28]. C. Moreno[27] 运用解析方法证明了上述定理只需假设两个整体表示在适当的有限多个有限位上有局部同构即可.

§5 四元数群的表示

设 F 是特征不为 2 的域. 我们给定 F 中两个元素 a 和 b, 以 $F\{a,b\}$ 表由 i 和 j 生成的 F 上的 4 次代数，其中 i 和 j 满足关系

$$i^2=a,\quad j^2=b,\quad 以及\ ij=-ji.$$

$F\{a,b\}$ 是一个中心为 F 的单代数.

例 1 设 $F=\mathbf{R}$, $a=b=-1$. 则 $\mathbf{R}\{-1,-1\}$ 是通常所说的 Hamilton 四元数代数.

例 2 设 $a=1, b=-1$. 令

$$i=\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix},\quad j=\begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix},$$

则

$$i^2=\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix},\quad j^2=\begin{pmatrix}-1 & 0\\ 0 & -1\end{pmatrix},\quad ij=\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}=-ji.$$

于是 $F\{1,-1\}$ 同构于矩阵代数 $\mathrm{M}_2(F)$.

一般地，可以证明，如果 $F\{a,b\}$ 含有一个非平凡零因子，那么它同构于矩阵代数 $\mathrm{M}_2(F)$; 否则，如果任何非零元都有乘法逆元素，我们称 $F\{a,b\}$ 为**四元数代数**，其非零元构成的乘法群称为 F 上的**四元数群**. 当 F 是一个局部域且 $F\neq \mathrm{C}$ 时，在同构意义下，只有唯一的一个四元数代数.

接下来考虑 F 是整体域， $a,b\in F^\times$ 时的情况. 此时，对 F 的任意位 v, a 和 b 都在完备化 F_v 里. 于是我们有了 $F\{a,b\}$ 和 $F_v\{a,b\}$. 显然，若 $F\{a,b\}$ 同构于 $\mathrm{M}_2(F)$, 则每个 $F_v\{a,b\}$ 同构于 $\mathrm{M}_2(F_v)$. 另一方面，若 $F\{a,b\}$ 是四元数代数，则 $F_v\{a,b\}$ 既可能是也可能不是四元数代数. 这可以由下面定义的 Hilbert 符号 $(a,b)_v$ 来刻画:

$$(a,b)_v=\begin{cases}1, & \text{若 } ax^2+by^2=z^2 \text{ 在 } F_v \text{ 中有非平凡解;}\\ -1, & \text{其他情况.}\end{cases}$$

习题 8 证明 $ax^2+by^2=z^2$ 在 F_v 中有非平凡解的充要条件是

$$a\in \mathrm{N}_{F_v(\sqrt{b})/F_v}(F_v(\sqrt{b})),$$

这等价于

$$b\in \mathrm{N}_{F_v(\sqrt{a})/F_v}(F_v(\sqrt{a})).$$

可以证明， $(a,b)_v=-1$ 的充要条件是 $F_v\{a,b\}$ 是一个四元数代数. 此时，我们称四元数代数 $F\{a,b\}$ 在位 v 处分歧. 由于只有有限多个位 v 使得 $(a,b)_v\neq 1$, 并且有积公式

$$\prod_v (a,b)_v=1,\quad v \text{ 过 } F \text{ 的位集}$$

成立，所以我们断言 $F\{a,b\}$ 在偶数个位上分歧. 反过来，给定一个整体域 F 和由偶数个 F 的位组成的有限集 S, 且 S 不包含任何 F 的复位，那么在同构意义下恰好存在一个 F 上的四元数代数，它在 S 中的位上分歧，而在 S 外的位上非分歧. 例如，Hamilton 代数 $\mathbf{Q}\{-1,-1\}$ 在位 ∞ 和 2 上分歧，在其他位上非分歧.

习题 9 利用上述讨论，证明:

(1) 若 a 是 F 中的平方元，则 $F\{a,b\}$ 同构于 $\mathrm{M}_2(F)$;

(2) 若 $F\{a,b\}$ 是四元数代数，则存在 F 的一个二次域扩张 L, 使得

$$F\{a,b\}\bigotimes_F L=L\{a,b\}$$

同构于 $\mathrm{M}_2(L)$;

(3) 若 H 是局部域 F 上的四元数代数，则在同构意义下，H 包含了 F 的所有二次扩张.

设 $H=F\{a,b\}$ 是 F 上基为 $1,i,j$ 和 ij 的四元数代数，其中 $i^2=a$, $j^2=b$, 以及 $ij=-ji$. 在 H 上有一个对合"—", 它映 $x=\alpha+\beta i+\gamma j+\delta ji$ 为 $\overline{x}=\alpha-\beta i-\gamma j-\delta ji$.

习题 10 证明：对任意的 $x,y\in H$, 和 $\alpha,\beta\in K$, 有

$\overline{\alpha x+\beta y}=\alpha\overline{x}+\beta\,\overline{y}$,	即对合为 K 线性的;
$\overline{xy}=\overline{y}\overline{x}$,	即对合为 H 的反自同态;
$\overline{\overline{x}}=x$,	即对合为 2 阶的.

由此，对合给出了 H 上的 F 线性的反自同构.

利用对合，我们可以定义 H 上的**简约范数** Nrd 和**简约迹** Trd 为：对 $x=\alpha+\beta i+\gamma j+\delta ji$, 有

$$\mathrm{Nrd}\ x=x\overline{x}=\overline{x}x=\alpha^2-\beta^2a-\gamma^2b+\delta^2ab\in F;$$
$$\mathrm{Trd}\ x=x+\overline{x}=2\alpha.$$

显然，Nrd 是由 $H^\times$ 到 $F^\times$ 的乘法同态，Trd 是 H 到 F 的一个加法同态. 选取一个 F 的二次扩张 $L=F(\sqrt{a})$. 利用将 i 映为

$\begin{pmatrix} \sqrt{a} & 0 \\ 0 & -\sqrt{a} \end{pmatrix}$, 将 j 映为 $\begin{pmatrix} 0 & b \\ 1 & 0 \end{pmatrix}$, 于是

$$x = \alpha + \beta i + j(\gamma + \delta i)$$

被映为

$$\begin{pmatrix} \alpha + \beta\sqrt{a} & b(\gamma - \delta\sqrt{a}) \\ \gamma + \delta\sqrt{a} & \alpha - \beta\sqrt{a} \end{pmatrix}.$$

这样我们把 $H = F\{a,b\}$ 嵌入到 $\mathrm{M}_2(L)$ 中去. 容易验证, $\mathrm{Trd}\ x$ 和 $\mathrm{Nrd}\ x$ 恰好是 x 所对应矩阵的迹和行列式.

设 F 是具备正规化赋值 $|\ |_F$ 的非 Archimedes 局部域, H 是 F 上的四元数代数. 则 $|\ |_F$ 可以扩充成 H 上的赋值 $|\ |_H$, 即

$$|x|_H = |\mathrm{Nrd}\ x|_F^{1/2}, \quad x \in H.$$

将 H 中赋值不大于 1 的元素全体记作 $\mathcal{O}_H$; $\mathfrak{p}_H$ 表示那些赋值 < 1 的元素全体. 则 $\mathfrak{p}_H$ 是 $\mathcal{O}_H$ 中唯一的极大理想, 并且它还是主理想. 进而, $\mathcal{O}_H$ 包含 F 的整数环 $\mathcal{O}_F$, $\mathfrak{p}_H$ 包含 $\mathfrak{p}_F$, 而且 $\mathcal{O}_H/\mathfrak{p}_H$ 是 $\mathcal{O}_F/\mathfrak{p}_F$ 的次数为 2 的域扩张. 与 F 类似, $\{\mathfrak{p}_H^n\}_{n\geq 1}$ 是 H 中 0 的一个邻域系, $\mathcal{O}_H$ 是即开又紧的. H 中的单位群是

$$\mathcal{U}_H = \mathcal{O}_H - \mathfrak{p}_H,$$

并且 $\{1+\mathfrak{p}_H\}$ 是 $H^\times$ 中 1 的邻域系, 记 $H^\times$ 为 $D(F)$. 则 $D(F)$ 的中心为

$$\mathcal{Z}'(F) \cong F^\times,$$

且 $D(F)/\mathcal{Z}'(F)$ 是紧的. 因此 $D(F)$ 的光滑表示是核为 $D(F)$ 的一个开子群的一个有限维表示, 且它是可容许的. 我们将研究 $D(F)$ 的可容许不可约表示. 对 $D(F)$ 中任一元 x, 以 $\mathrm{ord}_H x$ 表示使得 x 落在 $\mathfrak{p}_H^n$ 中的最小整数 n.

取 F 的一个零阶加法特征标 ψ. 设 $\mathrm{d}_H x$ 是 H 的关于加法特征 $\psi \circ \mathrm{Trd}$ 自对偶的 Haar 测度. 命

$$\mathrm{d}_D x = |\mathrm{Nrd}\ x|_F^{-1} \mathrm{d}_H x,$$

它是 $D(F)$ 的 Haar 测度. 对 $D(F)$ 的一个可容许不可约表示 ρ 和 $F^{\times}$ 的拟特征标 χ, 考虑下面形式幂级数

$$\sum_{n\in\mathbf{Z}}\left(\int_{\substack{x\in D(F)\\ \mathrm{ord}_H x=n}}\rho(x)\chi(\mathrm{Nrd}\ x)\psi(\mathrm{Trd}\ x)\mathrm{d}_D x\right)U^n.$$

由于 Trd 和 Nrd 是类函数, 所以对所有的 $g\in D(F)$, 每个 U^n 的系数在 $\rho(g)$ 的共轭作用 (即左右分别乘以 $\rho(g)$ 和 $\rho(g^{-1})$) 下不变. 又因 ρ 是不可约的, 所以利用 Schur 引理可知, 每个 U^n 的系数是一个纯量算子, 我们形式地记作

$$-\gamma_\rho(\chi,\psi,U)\mathrm{id}=\int_D\rho(x)\chi(\mathrm{Nrd}\,x)\psi(\mathrm{Trd}\,x)U^{\mathrm{ord}\,x}\mathrm{d}_D x,$$

其中 γ_ρ 是 U 的 Laurent 级数. 对上式两边取迹得:

$$\gamma_\rho(\chi,\psi,U)=-\int_D c_\rho(x)\chi(\mathrm{Nrd}\ x)\psi(\mathrm{Trd}\ x)U^{\mathrm{ord}\,x}\mathrm{d}_D x,\qquad(5.1)$$

其中 $c_\rho=\mathrm{Trd}\,\rho/\deg\rho$ 称为 ρ **的简约迹**. 通过直接计算可以证明, 如果 ρ 是一维的, 那么存在 $F^{\times}$ 的一个拟特征标 ξ, 使得 $c_\rho=\xi\circ\mathrm{Nrd}$, 并且

$$\gamma_\rho(\chi,\psi,U)=(q-1)^2q^{-2}\Gamma(\xi\chi,\psi,q^{-1}U)\Gamma(\xi\chi,\psi,U);$$

如果 ρ 的次数 ≥ 2, 那么 $\gamma_\rho(\chi,\psi,U)$ 是 U 的一个单项式. 因此 $\gamma_\rho(\chi,\psi,U)$ 可以视为 $\mathcal{A}(F^{\times})$ 中至多有一个极点的有理函数.

ρ 在 $D(F)$ 的中心 $\mathcal{Z}'(F)$ 上的限制是 $F^{\times}$ 的一个拟特征标 η. 设 c 是 $D(F)$ 上的一个函数. 下面三条性质给出了 c 是 $D(F)$ 的一个中心特征标为 η 的可容许不可约表示 ρ 之简约迹的判别条件:

(1) c 是 $D(F)$ 上的局部常值类函数;

(2) c 是 η 型的, 即对任意的 $u\in\mathcal{Z}'(F)$, $x\in D(F)$, 有

$$c(ux)=\eta(u)c(x);$$

(3) 对任意的 $x,y\in D(F)$, c 满足函数方程:

$$\int_{D(F)/\mathcal{Z}'(F)}c(xzyz^{-1})\mathrm{d}^{\times}z=c(x)c(y),$$

这里 $\mathrm{d}^\times z = \mathrm{d}_D x/\mathrm{d}^* x$, 而 $\mathrm{d}^* x$ 则是使得 $\mathcal{U}_F$ 的测度为 1 的 $F^\times$ 上的 Haar 测度.

我们更深入地讨论 $D(F)$ 上的类函数. 如果 $D(F)$ 中两个元素有相同的简约迹和简约范数, 则我们称它们为**共轭的**. 换句话说, $D(F)$ 的共轭类可以被映射

$$(\mathrm{Nrd},\ \mathrm{Trd}) : D(F) \to F^\times \times F$$

的像所参数化. 一个 $F^\times \times F$ 中的元素 (v, τ) 不在此像里的充要条件是它为双曲的, 即方程

$$x^2 - \tau x + v = 0$$

在 F 中有两个不同的解. 于是, 我们可把 $D(F)$ 的类函数 c 视为在双曲元素处为 0 的 $F^\times \times F$ 上的函数. 由此 $\gamma_\rho(\chi, \psi, U)$ 可被视为 c_ρ 的 Fourier 变换. 进一步, 在 (5.1) 式中把 c_ρ 换成 c, 则当且仅当由 (5.1) 式定义的函数 $\gamma_\rho(\chi, \psi, U)$ 满足乘积公式 (MF) (参见 §2) 时, 类函数 c 满足条件 (3). 特别地, 从必要性可得一个从 $D(F)$ 的可容许不可约表示的等价类到 $\mathrm{GL}_2(F)$ 的无限维可容许不可约表示的对应, 且对应的表示有相同的 γ 函数. 由于 $\gamma_\rho(\chi, \psi, U)$ 至多有一个极点, 所以这一对应的像含于 $\mathrm{GL}_2(F)$ 的离散序列表示集里. 事实上, 这个像恰好是 $\mathrm{GL}_2(F)$ 的所有离散序列表示集. 从比较各自的 γ 函数可以看到, 一个 $\mathrm{GL}_2(F)$ 的特殊表示

$$\pi = \sigma(\mu|\ |, \mu)$$

对应了 $D(F)$ 的一个次数为 1 的表示 $\mu|\ |^{-1/2} \circ \mathrm{Nrd}$. 对超尖点表示 π, 利用在 (5.1) 式给出的 Fourier 变换, 不过这里要把 γ_ρ 换成 γ_π, 我们可以得到 $F^\times \times F$ 上的一个局部常值函数 c. 从 γ_π 是单项式并满足 (MF) 式可知, c 在双曲元素处为 0, 于是它可以视为 $D(F)$ 上满足条件 (1) 和 (2) 的类函数. 又因函数 γ_π 满足 (MF) 式, 所以条件 (3) 也满足. 这表明 $c = c_\rho$. 总结上面讨论, 我们得到

定理 13 *设 F 是一个非 Archimedes 局部域, $\gamma(\chi, \psi, U)$ 是 $\mathcal{A}(F^\times)$ 上的有理函数. 则存在 $D(F)$ 的一个中心特征标为 η 的可*

容许不可约表示 ρ, 使得 $\gamma=\gamma_\rho$ 成立的充分必要条件是: γ 至多有一个极点, 并满足具有同样特征标 η 的 (MF) 式. 进而 γ_ρ 决定 ρ 的简约迹.

再结合定理 3, 就得到了

定理 14 (局部对应) 设 F 是一个非 Archimedes 局部域. 则存在一个从 $D(F)$ 的可容许不可约表示的等价类到 $\mathrm{GL}_2(F)$ 的无限维可容许不可约表示的对应, 使得对应的表示有相同的 γ 函数. 更细致些, $D(F)$ 的次数为 1 的表示对应了 $\mathrm{GL}_2(F)$ 的特殊表示; $D(F)$ 的次数 ≥ 2 的表示对应了 $\mathrm{GL}_2(F)$ 的超尖点表示.

定理 14 的第一个结论对 $F=\mathbf{R}$ 的情况也是成立的. 关于定理 13 和定理 14 的详尽讨论, 读者可以参阅参考文献 [14], [15].

尽管局部域 F 上一个四元数群 $D(F)$ 的可容许不可约表示 ρ 没有 Whittaker 模型, 但对 F 的非平凡加法特征标 ψ, 我们仍可定义函数 $L(\rho,s)$ 和 $\varepsilon(\rho,\psi,s)$. 类似于 GL_1 的情形, 它们可以从结合 ρ 的矩阵系数和 F 上四元数代数上的 Schwartz 函数的局部 zeta 函数得到. 同结合 Whittaker 模型的积分类似, 这些局部 zeta 函数也有解析开拓和含有 L 因子和 ε 因子的函数方程. 特别地,

$$\gamma_\rho(\chi,\psi,s)=\frac{L(\check{\rho}\bigotimes\chi^{-1},1-s)}{L(\rho\bigotimes\chi,s)}\varepsilon(\rho\bigotimes\chi,\psi,s),$$

其中, 当 F 是一个剩余类域的势为 q 的非 Archimedes 局部域时, 用 $\gamma_\rho(\chi,\psi,s)$ 代表 $\gamma_\rho(\chi,\psi,q^{-s})$.

现在研究 F 是整体域时的情况. 设 H 是 F 上的四元数代数. 记 D 为四元数群 $H^\times$, Z' 是 D 的中心. 在一个使 H 分歧的位 v 处, $D(F_v)$ 是四元数群, 而在使 H 非分歧的位 v 处, $D(F_v)$ 同构于群 $\mathrm{GL}_2(F_v)$. 固定这些局部同构. 在非 Archimedes 位 v 处令

$$D(\mathcal{O}_v)=\begin{cases}\mathrm{GL}_2(\mathcal{O}_v), & \text{若 } H \text{ 在 } v \text{ 处非分歧;}\\ D(F_v)\text{ 的单位群}, & \text{若 } H \text{ 在 } v \text{ 处分歧.}\end{cases}$$

定义阿代尔群 $D(A_F)$ 为 $\{D(F_v)\}$ 关于 $\{D(\mathcal{O}_v)\}$ 的限制直积. 在

分歧位 v 处, 以 Nrd_v 表简约范数; 而在非分歧位 v 处, Nrd_v 则是行列式映射. 于是 Nrd_v 是一个从 $D(F_v)$ 到 $F_v^\times$ 的同态. 定义**整体简约范数** Nrd 是从 $D(A_F)$ 到 I_F 的同态, 它映 $x=(x_v)\in D(A_F)$ 为 $\mathrm{Nrd}\,x=(\mathrm{Nrd}_v x_v)\in I_F$.

设 η 是伊代尔类群 $I_F/F^\times$ 的一个拟特征标. $D(A_F)$ 上的函数 f 若满足

(1) 对任意的 $\gamma\in D(F)$, $g\in D(A_F)$, 和 $z\in \mathcal{Z}'(A_F)$, 有

$$f(\gamma g z)=\eta(z)f(g);$$

(2) f 是右 $\mathcal{K}$ 有限的, 其中

$$\mathcal{K}=\prod_v \mathcal{K}_v$$

是 $D(F_v)$ 的标准最大紧子群 $\mathcal{K}_v$ 的积, 则称 f 是 $D(A_F)$ 上**中心特征标为 η 的自守形式**. 注意, 由于 $D(F)\setminus D(A_F)/\mathcal{Z}'(A_F)$ 是紧的, 所以这里可以不加增长条件的限制. 记这些自守形式的空间为 $\mathcal{A}(D(A_F),\eta)$. 对 $D(A_F)$ 的一个可容许不可约表示, 如果存在特征 η, 使得它是 $D(A_F)$ 在 $\mathcal{A}(D(A_F),\eta)$ 上的正则表示的一个组成份子, 则称它是**自守表示**.

对 $D(A_F)$ 的一个可容许不可约表示 π', 它或者是一维的, 即存在 $I_F/F^\times$ 的拟特征标 ω, 使得 $\pi'=\omega\circ\mathrm{Nrd}$; 或者是无限维的. 当 π' 是无限维时, 它是 $D(F_v)$ 的局部可容许不可约表示 π_v' 的限制张量积 $\bigotimes_v' \pi_v'$. 若在位 v 处 H 非分歧, 则 $D(F_v)$ 同构于 $\mathrm{GL}_2(F_v)$, 且 π_v' 是无限维的; 若在位 v 处 H 分歧, 则 $D(F_v)/\mathcal{Z}'(F_v)$ 是紧的, 因此 π_v' 是有限维的. 每个 π_v' 都结合了 L 因子和 ε 因子. 定义

$$L(\pi',s)=\prod_v L(\pi_v',s),\quad \varepsilon(\pi',s)=\prod_v \varepsilon(\pi_v',\psi_v,s),$$

其中 $\psi=\prod_v \psi_v$ 是在 F 上平凡的一个 A_F 的非平凡加法特征标. 用 $H(A_F)$ 上的 Schwartz 函数可定义 π' 结合的整体 zeta 函数. 利

用这个 zeta 函数，Jacquet 和 Langlands[17] 给出结合 π' 以及结合其逆步表示 $\widetilde{\pi}'$ 的 L-函数的解析性质，即

定理 15(整体函数方程) 设 F 是整体域，π' 是 $D(A_F)$ 的无限维可容许不可约自守表示. 则 $L(\pi',s)$ 和 $L(\widetilde{\pi}',s)$ 在整个 s 平面上有全纯开拓，它们满足函数方程

$$L(\pi',s)=\varepsilon(\pi',s)L(\widetilde{\pi}',1-s),$$

并且，当 F 是数域时，它们在任意有限宽的竖带区域中有界；当 F 是一个常数域的势为 q 的函数域时，它们是 q^{-s} 的多项式.

设 χ 是 $I_F/F^{\times}$ 的伊代尔类特征标，显然，π' 被 χ 扭曲后结合的 L-函数也有与上面结论相同的性质. 从定理 14 和定理 12 看出，存在一个 $\mathrm{GL}_2(A_F)$ 的可容许不可约尖点表示 $\pi=\bigotimes_v'\pi_v$，使得在 H 非分歧的位 v 处，$\pi_v=\pi_v'$；而在 H 分歧的位 v 处，π_v 和 π_v' 满足局部对应. 于是对任意的 $I_F/F^{\times}$ 的拟特征标 χ 有

$$L(\pi\bigotimes\chi,s)=L(\pi'\bigotimes\chi,s).$$

这就导出了一个从 $D(F)$ 的无限维可容许不可约自守表示的等价类集到可容许不可约尖点表示类集的单射，其中，这些尖点表示在使 H 分歧的位处的分支是离散序列表示. 利用迹公式，S. Gelbert 和 H. Jacquet[12] 证明这个单射同时也是个满射. 总结一下，就是下述定理.

定理 16(整体对应) 设 F 是整体域，H 是 F 上的四元数代数，$D=H^{\times}$. 用 S 表示 F 的那些使 H 在该位处分歧的位集. 则存在一个从 $D(A_F)$ 的中心特征标为 η 的无限维可容许不可约自守表示的等价类集到 $\mathrm{GL}_2(A_F)$ 的中心特征标为 η 的可容许不可约尖点表示类集的一个双射，其中，这些尖点表示在 S 中的位处的局部分支是离散系列表示. 并且，若

$$\pi'=\bigotimes_v{}'\pi_v'$$

是 $D(A_F)$ 的一个这样的表示，$\pi=\bigotimes_v'\pi_v$ 是对应的 $\mathrm{GL}_2(A_F)$ 的

表示，则当位 $v \notin S$ 时，π_v 与 π'_v 同构；当位 $v \in S$ 时，π_v 与 π'_v 有一个局部对应. 特别地，对任意的 $I_F/F^\times$ 的拟特征标 χ，有

$$L(\pi' \otimes \chi, s) = L(\pi \otimes \chi, s), \quad \varepsilon(\pi' \otimes \chi, s) = \varepsilon(\pi \otimes \chi, s).$$

当 H 跑遍域 F 上的所有四元数代数时，在上述整体对应下的所有的像之并恰好是群 $\mathrm{GL}_2(A_F)$ 的所有中心特征标为 η 且至少有两个局部分支是离散序列表示的可容许不可约尖点表示全体.

参考文献

[1] J. Arthur, *Automorphic representations and number theory*, Canad. Math. Soc. Conf. Proc. 1. Amer. Math. Soc., Providence, 1981 3~54.

[2] S. Birch and D. Zagier, *Modular Forms of One Variable*, V, VI, Lecture Notes in Mathematics, 601, 627, Springer-Verlag, Berlin 1975, 1976.

[3] A. Borel and W. Casselman, *Automorphic forms, representations, and L-functions*, Proc. Symp. Pure Math., vol. 33, Parts 1, 2, Amer. Math. Soc., Providence, 1979.

[4] A. Borel and H. Jacquet, *Automorphic forms on automorphic representains*, In [3] Part 1, 189-202.

[5] A. Borel and G. Mostow, *Algebraic groups and discontinuous subgroups*, Proc. Sympos. Pure Math., vol. 9, Amer. Math. Soc., Providence, 1966.

[6] H. Carayol, *Représentations cuspidales du groupe linéaire*, Ann. Scien. École. Norm. Sup., **17** (1984), 191~225.

[7] P. Deligne, *Formes modulaires et représentations de* GL(2), In [8] II, Lecture Notes in Math., **349** (1973), 55~105.

[8] P. Deligne and W. Kuyk, *Modular Forms of One Variable*, I–IV, Lecture Notes in Mathematics, 320, 349, 350, 476, Springer-Verlag, Berlin 1973, 1974.

[9] D. Flath, *Decomposition of representations into tensor products*, In [3] Part 1, 179~183.

[10] S. Gelbart, *Automorphic Forms on Adele Groups*, Princeton University Press, 1975.

[11] S. Gelbart, *An elementary introduction to the Langlands program*, Bull. Amer. Math. Soc., **10** (1984), 471~552.

[12] S. Gelbart and H. Jacuqet, *Forms of* GL(2) *from the analytic point of view*, In [3] Part 1, 213~251.

[13] I. Gelfand, M. Graev and I. Pyatetskii-Shapiro, *Representation Theory and Automorphic Functions*, Saunders Co., Phliladephia, 1969.

[14] P. Gérardin and W.-C. W. Li(李文卿), *A functional equation for degree two local factors*, Canad. Math. Soc. Bull., **28** (1985), 355~371.

[15] P. Gérardin and W.-C. W. Li(李文卿), *Fourier transforms of representations of quaternions*, J. reine angewandte Math., **359** (1985), 121~173.

[16] H. Jacquet, *Les fonctions de Whittaker associees aux groupes de Chevalley*, Bull. Soc. Math. France, **95** (1967), 243~309.

[17] H. Jacquet and R. P. Langlands, *Automorphic Forms on* GL(2), Lecture Notes in Math., 114, Springer-Verlag, Berlin, 1970.

[18] A. A. Kirillov, *Elements of the Theory of Representations*, Springer-Verlag, Berlin, 1976.

[19] P. Kutzko, *On the supercuspidal representations of* GL_N *and the otherp-adic groups*, Proc. Int. Cong. Math., 1986, Amer. Math. Soc., Providence, R. I. 1987, 853~861.

[20] P. Kutzko and D. Manderscheid, *On the supercuspidal representations of* GL_N, *N the product of two primes* Ann. Sci. École Norm. Sup., **23** (1990), 89~121.

[21] 黎景辉 (K. F. Lai)、蓝以中，《二阶矩阵群的表示与自守形式》，北京大学出版社，北京，1990.

[22] S. Lang, SL(2,**R**), GTM 105, Springer-Verlag, New York, 1989.

[23] R. P. Langlands, *Problems in the theory of automorphic forms*, Lecture Notes in Mathematics 170. Springer-Verlag, Heidelberg, 1970, 18~61.

[24] 李文卿 (W.-C. W. Li), *Barnes identities and representations of* GL_2. Part II:

Nonarchimedean local field case, J. reine angewanddte Math., **345** (1983), 69~92.

[25] 李文卿 (W.-C. W. Li), *On converse theorems for* GL(2) *and* GL(1), Amer. J. Math., **103** (1980), 851~885.

[26] G. Mackey, *Unitary Representations in Physics, Probability and Number Theory*, Benjamin/Cummings, Reading, Mass., 1978.

[27] C. Moreno, *Analytic proof of the strong multiplicity one theorem*, Amer. J. Math., **107** (1985), 163~206.

[28] I. Piatetski-Shapiro, *Multiplicity one theorems*, In [3] Part 1, 209~212.

[29] A. Selberg, *Harmonic analysis and discontinuous groups in weakly symmetric Remannian spaces with applications to Dirichlet series*, Jour. Indian Math. Soc., **20** (1956), 47~87.

[30] J. A. Shalika, *The multiplicity one theorem for* GL(n), Ann. of Math., **100** (1974), 171~193.

[31] M. Sugira, *Unitary Representation and Harmonic Analysis——An Introduction*, Kodansha, 1975.

[32] J. Tate, *Fourier analysis in number fields and Hecke's zeta functions*, Thesis, Princeton University, 1950: Published in *Algebraic Number Theory*, J. W. S. Cassels and A. Fröhlich edal, Thompson, Washington D. C. 1967, republished by Academic Press, London, 1989.

[33] A. Terras, *Harmonic Analysis on Symmetric Spaces and Applications*, I, II, Springer- Verlag, New York, 1985, 1988.

[34] M.-F. Vigneras, *Arithmetique des Algebres de Quaternions*, Lecture Notes in Math., 800, Springer-Verlag, Heidelberg, 1980.

[35] V. S. Varadarajan, *Lie Groups, Lie Algebras and their Representations*, GTM 102, Springer-Verlag, New York, 1984.

[36] N. Wallach, *Representations of reductive Lie groups*, In [3], Part 1, 71~86.

[37] A. Weil, *Dirichlet Series and Automorphic Forms*, Lecture Notes in Math., 189, Springer-Verlag, Berlin, 1979.

[38] 严志达、许以超，《李群及其李代数》，高等教育出版社，北京， 1985.

第九章　应　　用

这一章的目的是向读者描述如何把前八章所讨论的数论结果用于解决现实生活中的实际问题. 我们所讨论的问题是从通讯网络中产生的: 在一定经费条件限制下, 如何建立一个效率高的网络. 本章要求读者具备一定的图论知识, 对于不熟悉图论的读者, 可以参阅有关书籍. 由于图论的参考文献很多, 所以我们在此就不推荐参考书目了.

§1　扩展图, Kazhdan 性质 T 和特征值

一个通讯网络可以用一个有限图 G 来表示. 一个有效的网络意味着它可以把从一个顶点发出的信息很快地传送到全部网络上. 如何用数学来刻画此事呢? 我们知道电讯号的传送速度非常快, 因此影响信息传送的主要因素是途中所经过的中转站 (即图 4 中的顶点) 的接收与发送, 所以, 两点间传送信息的速度主要依赖于两点间中转站的数目. 当向整个网络传送信息时, 一个好的网络应该是每一站都能向尽可能多的其他站发送信息, 用图论的话说, 就是图中的每个顶点有尽可能多的邻点. 例如图 5 所代表的网络中, 当我们从 A 点发出信息时, 要达到全部网络需要 4 次传送,

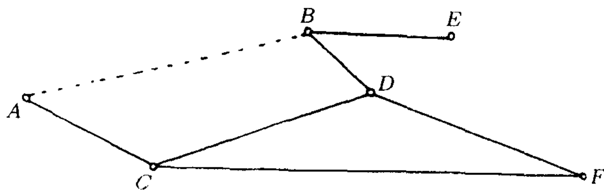


图　5

但如果把 A 和 B 点联结起来，则至多只需两次传送即可把从 A 点传出的信息发到网络中的任何一点. 于是，为了反映网络的有效性，我们引入一个伸缩系数的概念：对图 G 的一个顶点集 X, 定义它的边界 ∂X 为在 X 之外，且与 X 中的某些点相邻的顶点集. 图 G 的**伸缩系数**定义为

$$c = \min_X \frac{|\partial X|}{|X|},$$

其中 X 跑遍 G 的所有不超过 G 的一半的顶点子集. 对一个有 n 个顶点的完备图 G,

$$c = \begin{cases} 1, & \text{若 } n \text{ 是偶数}, \\ (n+1)/(n-1), & \text{若 } n \text{ 是奇数}. \end{cases}$$

不过在一般情况下，我们基本上总有 $0 \le c \le 1$. 若 G 有 n 个顶点，每个顶点至多有 k 个邻点，则对任意的 $0 \le c' \le c$, 我们称 G 是一个 (n,k,c')-**扩展图**.

尽管当网络是一个完全图时信息的传送是非常有效的，但它即不经济也不现实. 事实上，对固定的顶点数 n 和最大邻点数 k, 我们希望找到那些具有大的伸缩系数 c 的扩展图. 或更好一些，构造无限多个具有相同的 k 和很大的伸缩系数的扩展图. 一般而言，如果一个图是一个随机图，那么它的伸缩系数通常是比较好的. 然而，确定一个图的伸缩系数是一件非常困难的事情. 因此，精确构造好的扩展图是十分有意义的. 在过去的 20 年中，产生了两种系统构造扩展图的方法. 在此我们简单地概述一下.

第一种方法是用 Kazhdan 性质 T. 对一个局部紧群 Γ, 如果它的平凡表示孤立于它的其他酉表示，则我们称群 Γ 有 **Kazhdan 性质** T. 衡量平凡表示与其他表示的差距，我们采用一种所谓的 **Kazhdan 常数** κ. 表示的拓扑类似于"紧开"拓扑，其中群 Γ 的生成元集扮演了紧集的角色. 因此，平凡表示与其他表示的差距，即 κ, 仅依赖于 Γ 的生成元的选取.

利用 Kazhdan 性质 T 来构造扩展图是由 Margulis 在 1975 年

首先提出的. 在参考文献 [19] 中, 他利用 $\Gamma = \mathrm{SL}_2(\mathbf{Z}) \ltimes \mathbf{Z}^2$ 来构造邻点数 $k=5$, 伸缩系数 $=\kappa^2/2$ 的偶图, 其中 κ 是从 Γ 的四个生成元产生的 Kazhdan 常数, 这 4 个生成元是用来定义他的这个图的. 可惜的是, 他没能算出 κ. 1981 年, Gabber 和 Galil[12] 采用同样的方法但选取了另外 4 个生成元构造了一类新的 $k=5$ 的图, 并且他们成功地算出伸缩系数. 从那以后, 又有了一些类似的构造改进了伸缩系数.

第二种方法是借助于 G 上 Laplace 算子的最小正特征值 λ_1. 更精确地讲, 视 G 为一个一维单复形. 以 $C^0(G)$ 表示 G 的顶点的函数空间, $C^1(G)$ 表示 G 的边的函数空间. 定义一个由 $C^0(G)$ 到 $C^1(G)$ 的线性映射 d 为

$$(df)(e) = f(e^+) - f(e^-), \quad e \text{ 是 } G \text{ 的任意一条边}.$$

这里, 我们对每条边选择了一个方向, e^+ 和 e^- 分别表示边 e 的终点和起点. 我们用 d^* 表示映射 d 的伴随映射, 在我们这种情况它恰为 d 的转置. Laplace 算子 Δ 定义为 d^*d. 由简单的计算可以很容易地看出, 如果我们取 G 的顶点的特征函数为 $C^0(G)$ 的基, 那么 Δ 可以用 $D-A$ 来表示, 其中 D 和 A 均为方阵, 它们的元素是由 G 的顶点所决定的: D 称为 G 的**次数矩阵**, 它是一个对角矩阵, 其对角元素是 G 的顶点的邻点的个数 (称为**次数**); A 被称为**邻接矩阵**, 其 xy 处的元素恰为由顶点 x 到 y 的边的个数.

习题 1 设 $\mathcal{F}(G)$ 为定义在 G 的顶点上的实值函数空间. 则 A 可视为 $\mathcal{F}(G)$ 上的线性算子

$$(Af)(x) = \sum_y f(y),$$

其中 y 跑遍 G 中所有 x 的邻点.

特别需要指出的是 Δ 不依赖于 G 上边的方向的选取. 设 f 是 Δ 的一个特征函数, 特征值是 λ, 则利用 $C^0(G)$ 上的内积 $\langle\ ,\ \rangle$, 由

$$\lambda\langle f,f\rangle = \langle \Delta f, f\rangle = \langle df, df\rangle$$

可得 $\lambda \geq 0$. 由于常值函数是特征值为 0 的特征函数，因此我们可以将 G 的 n 个特征值排列如下

$$0 = \lambda_0 \leq \lambda_1 \leq \cdots \leq \lambda_{n-1},$$

这里 n 是图 G 的顶点个数. 假定 G 是连通的，则 0 是一个重数为 1 的特征值，故 $\lambda_1 > 0$.

Tanner 在 1984 年利用 λ_1 给出了伸缩系数 c 的一个下界:

定理 1[33] *假定每个顶点的次数都不超过 k. 则*

$$c \geq \frac{2\lambda_1}{k + 2\lambda_1}.$$

由此我们可以看出 λ_1 越大，G 的伸缩系数越大.

反过来，Alon 和 Milman 在 1985 年证明了 λ_1 有一个用 c 表达的下界:

定理 2[1] $\lambda_1 \geq \dfrac{c^2}{4 + 2c^2}$.

从上面的讨论可以看出，利用 Kazhdan 性质 T 的方法存在两个困难: 其一是它不能像定理 1 那样用 Kazhdan 常数 κ 给出伸缩系数 c 的界，其二是计算 κ 是很困难的. 因此第二种方法就更显得有效，特别是我们可以给出 λ_1 的界，从而就可以得到 c 的估计. 在 §4 里，我们将介绍几种构造具有很大 λ_1 的图的方法. 此外，Alon 和 Milman 找到了 λ_1 和 κ 之间的联系，我们现在解释一下. 设 Γ 是具有 Kazhdan 性质 T 的可数离散群，$S = S^{-1}$ 是由 Γ 的生成元构成的对称集. 用 κ 表示从 S 导出的 Kazhdan 常数. 设 $\overline{\Gamma}$ 是 Γ 的有限商群，$\overline{S}$ 是 S 在投射 $\Gamma \to \overline{\Gamma}$ 下的像. 图 G 取作具有生成元 $\overline{S}$ 的 Cayley 图 $\overline{\Gamma}$. 换句话说，G 的顶点是 $\overline{\Gamma}$ 中的元素，而 $x \in G$ 的邻点集为 $x\overline{S}$.

定理 3[1] $\lambda_1(G) \geq \kappa$.

这个定理可以视为对 κ 的一个上界估计，同时它也可以看成是构造一类有无限多个图的途径，这些图的最小非零特征值一致地受囿于一个下界. 有关这一节和下一节内容的更详细的讨论，读

者可参阅 Bien 的文章 [3] 和 Sunada 的文章 [31,32].

注释　关于流形的 Laplace 和 Kazhdan 性质 T

这一节的许多想法和结果均来自流形. 在此我们仅举两个例子. 设 M 是一个维数为 n 的紧 Riemann 流形. 与图的伸缩系数对应的是 M 上的 **Cheeger 系数**, 其定义如下:

$$c = \inf_S \frac{\text{area}\,(S)}{\min\big(\text{vol}\,(M_1),\ \text{vol}\,(M_2)\big)},$$

其中 S 跑遍 M 的这样一些 $(n-1)$-维子流形: 它把 M 分成两部分 M_1 和 M_2 且使得至少有一部分的体积有限 (此时, S 为 M_1 和 M_2 的公共边界). 上式中 S 的 "面积元" 由 M 的体积元导出.

流形 M 上的 Laplace 算子 Δ 同样也是用 d^*d 定义的, 其中 d 是可微函数上的微分算子在 M 上 L^2 函数上的推广; λ_1 定义为

$$\lambda_1 = \lambda_1(M) = \inf_f \frac{\displaystyle\int_M \|\mathrm{d}f\|^2}{\displaystyle\int_M |f|^2},$$

这里 f 跑遍 M 上所有垂直于常值函数的函数, 即

$$\int_M f = 0.$$

1970 年, Cheeger 证明了下面不等式:

定理 4[6]　$\lambda_1 \geq \dfrac{c^2}{4}$.

定理 2 中关于图的界与上面结论非常接近.

联系流形的 Kazhdan 性质 T, Brooks[4] 证明了下面这个与定理 3 类似的结果.

定理 5[4]　*设 M 是一个紧 Riemann 流形. 假定它的基本群 $\pi_1(M)$ 有 Kazhdan 性质 T, 则存在常数 $c>0$, 使得对 M 的任意有*

限覆盖 M', $\lambda_1(M') \geq c$.

§2 正则图的谱

首先，我们提醒读者，如无特殊说明，我们这里研究的图都是有向的，即每条边是有方向的. 对有向图的顶点，我们称进入这一点的边的条数是该点的**入次数**，由此点出发的边的条数为其**出次数**.

为了简单起见，我们仅考虑 **k-正则图**, 即，在每个顶点处，入次数 = 出次数 $=k$. k-正则图 G 的次数矩阵 D 为常数方阵 kI, 而 Laplace 算子 $\Delta = D - A$, 故

$$\lambda_1 = k - A \text{ 的第二大特征值}.$$

邻接矩阵 $A = A(G)$ 的特征值称为 G 的**谱**. 当 G 是 k-正则时，A 的每一行，每一列的元素加在一起均等于 k, 因此 k 是 A 的一个特征值，对应的特征函数是 G 上的常值函数. 它对应了 Laplace 算子 $\Delta = kI - A$ 的 0 特征值. 可以看出，$A(G)$ 的任何特征值 λ 满足 $|\lambda| \leq k$. 事实上，设 f 是 $A = A(G)$ 的一个有特征值 λ 的非平凡的特征函数，假定 f 的绝对值在顶点 x 处达到最大值，则 $f(x) \neq 0$. 进而,

$$\lambda f(x) = (Af)(x) = \sum_{x \to y} f(y).$$

对上式两边取绝对值得

$$|\lambda|\,|f(x)| \leq \sum_{x \to y} |f(y)| \leq k|f(x)|,$$

又因 $f(x) \neq 0$, 从而 $|\lambda| \leq k$.

对一个图 G, 若 G 的顶点可以分拆成 r 个不相交的点集 $V_1, \cdots, V_r$, 且对任意的 $i \in \mathbf{Z}/r\mathbf{Z}$, 由 V_i 中的点出发的边其终点一定在 V_{i+1} 中，则我们称这个图为 **r-可分的**. 假定 G 是 r-可分的，λ 是 G 的

一个特征值，f 是其对应的非平凡特征函数．设 ζ 是任意一个 r 次单位根．定义 G 的顶点函数 $\tilde{f}$ 为：在 V_i 中的顶点 x 上，定义 $\tilde{f}(x)=\zeta^i f(x)$．于是对任意的 $x\in V_i$，有

$$\begin{aligned}(A\tilde{f})(x)&=\sum_{x\to y}\tilde{f}(y)=\zeta^{i+1}\sum_{x\to y}f(y)\\&=\zeta^{i+1}(Af)(x)=\zeta^{i+1}\lambda f(x)=\zeta\lambda\tilde{f}(x).\end{aligned}$$

由于此式对所有的 $i\in\mathbf{Z}/r\mathbf{Z}$ 成立，所以我们就证明了 $\tilde{f}$ 是一个 A 的特征值为 $\zeta\lambda$ 的特征函数．

特别地，若 G 是 k-正则的 r-可分图，则对任意的 r 次单位根 ζ, ζk 是 $A(G)$ 的特征值．称 ζk 为 G 的**平凡特征值**，其余的为**非平凡**的．对一个 k-正则图 G，命

$$\lambda(G)=A(G)\text{ 的非平凡特征值的绝对值中的最大者}.$$

则 $\lambda(G)\ge k-\lambda_1$，现在的任务是构造具有小 $\lambda(G)$ 的 k-正则图．

$\lambda(G)$ 不仅与 G 的伸缩系数有关（我们将在 §8 里论述），而且它还反映了 G 的许多重要信息．例如，它给出了 G 的直径，即 G 中顶点间的距离的上界．若 G 代表一个通讯网络，则它的直径是传送延误的一种度量，更精确的描述是下面这个由 Chung 证明的定理：

定理 6[8] 设 G 是一个有 n 个顶点的无向的 k-正则图．则 G 的直径 $\le(\log n-1)\Big/\log\dfrac{k}{\lambda(G)}$．

因此 $\lambda(G)$ 越小，则图的直径越小．这给出了另一个我们为什么要构造具有小 λ 的正则图的原因．

$\lambda(G)$ 能够有多小呢？若 G 是 k-正则的，且邻接矩阵 $A=A(G)$ 可以被一个酉矩阵对角化，则 $A\,{}^tA$ 的迹是 nk 且 $A\,{}^tA$ 的特征值是 A 的特征值绝对值的平方．因此，如果 G 又是 r-可分的，则 $n\ge rk$ 且 $rk^2+(n-r)\lambda(G)^2\ge nk$，进而导出下面这个 $\lambda(G)$ 的平凡下界：

$$\lambda(G)\ge\left(\frac{n-rk}{n-r}\right)^{1/2}\sqrt{k}.$$

对无向图的一个非平凡下界是由 Alon 和 Boppana 给出的 (参见参考文献 [18]):

定理 7(Alon-Boppana) 对一个无向 k-正则图 G, 我们有

$$\liminf \lambda(G) \geq 2\sqrt{k-1}, \quad |G| \to \infty.$$

若 G 为一有向的 k-正则图, 其对应的矩阵 $A = A(G)$ 可以被酉矩阵对角化, 则同样的下界也成立. 这是因为无向偶图结合的邻接矩阵是 $\begin{pmatrix} 0 & A \\ {}^{t}A & 0 \end{pmatrix}$, 其特征值为 $\pm|\lambda|$, 其中 λ 跑遍 A 的所有特征值. 由上面定理看出, 若 $\lambda(G) \leq 2\sqrt{k-1}$, 则我们可以说 k-正则图 G 的特征值很小. 按照 Lubotzky–Phillips–Sarnak[18], 若图 G 满足

(1) G 是 k-正则的;

(2) $\lambda(G) \leq 2\sqrt{k-1}$;

(3) $A(G)$ 可被酉矩阵对角化.

则我们称 G 是 **Ramanujan 图**. 由于一个 k-正则 r-可分的 Ramanujan 图可以由无向 r-可分的 Ramanujan 偶图生成, 于是上面的定义可以包含有有向图.

注 对于一个无向图 G, 因为 $A(G)$ 是对称的, 故它可被正交矩阵对角化, 因此, 上述第三个条件自动满足. 另一方面, 当我们去掉 $A(G)$ 可被酉矩阵对角化这个条件而简单代之以 $A(G)$ 可被对角化这一条件时, 定理 7 不再成立. 事实上, 我们有下面由冯克勤、李文卿证明的结论:

定理[11] 给定整数 r 和 k. 则存在无限多个 k-正则、r-可分的有向图, 其邻接矩阵可对角化, 且它们的非平凡特征值均在单位圆中. 特别地, 当 G 跑遍所有邻接矩阵可对角化的 k-正则 r-可分图时,

$$\liminf_{|G|\to\infty} \lambda(G) = 1.$$

Ramanujan 图在通讯网络、极图理论, 以及计算复杂性等领域中有着广泛的应用. 虽然随意取出的一个 k-正则图有极大的可能

性是 Ramanujan 图，但是要验证一个图是否是 Ramanujan 图却是一件很困难的事. 因此，精确地构造 Ramanujan 图是十分必要的. 到目前为止，我们已有三种系统的方法来构造 Ramanujan 图，而且它们都是借助于数论方法产生的，我们将在 §3～§5 三节中逐个介绍.

§3 由四元数群构造 Ramanujan 图

在这一节中，我们所构造的 Ramanujan 图是一个 $(q+1)$-正则图，其顶点是一些四元数群的阿代尔点的双边陪集，其中，q 是一个素数或素数的幂. 利用 Hamilton 四元数群来构造 Ramanujan 图的想法可追溯到 Eichler 和 Brandt，但第一个采用此方法精确构造出 Ramanujan 图的是 Margulis[20]，而 Lubotzky, Phillips 和 Sarnak[18] 也独立地做出了同样的工作.

给定一个素数 p. 设 H 是 $\mathbf{Q}$ 上的四元数代数，且它在 ∞ 处分歧，在 p 处非分歧. 设 D 是 H 的乘法群. 设 $\prod\limits_q K_q$ 是 $D(A_{\mathbf{Q}}^f)$ 的标准最大紧子群的一个开同余子群，使得 $K_p = D(\mathbf{Z}_p)$ 且

$$\mathrm{Nrd}\Big(\prod_q K_q\Big) = \prod_q \mathcal{U}_q.$$

设 SD 为由 D 中简约范数为 1 的元素组成的子群，关于 SD 利用强逼近定理可得

$$D(A_{\mathbf{Q}}) = D(\mathbf{Q}) \cdot D(\mathbf{R})D(\mathbf{Q}_p)\prod_q K_q,$$

从而有下面关系

$$\begin{aligned}X =& D(\mathbf{Q})\backslash D(A_{\mathbf{Q}})/D(\mathbf{R})\prod_q K_q\mathcal{Z}'(A_{\mathbf{Q}})\\ \approx& \widetilde{\Gamma}\backslash D(\mathbf{Q}_p)/D(\mathbf{Z}_p)\mathcal{Z}'(\mathbf{Q}_p)\\ =& \widetilde{\Gamma}\backslash \mathrm{GL}_2(\mathbf{Q}_p)/\mathrm{GL}_2(\mathbf{Z}_p)\mathcal{Z}(\mathbf{Q}_p),\end{aligned}$$

其中 $\widetilde{\Gamma} = D(\mathbf{Q}) \bigcap \prod_{q \neq p} K_q$ 是

$$D\left(\mathbf{Z}\left[\frac{1}{p}\right]\right) = D(\mathbf{Q}) \bigcap \prod_{q \neq p} D(Z_q)$$

的同余子群，这里 $D\left(\mathbf{Z}\left[\frac{1}{p}\right]\right)$ 是 $D(\mathbf{Q}_p) = \mathrm{GL}_2(\mathbf{Q}_p)$ 的一个离散子群. 由于 H 在 ∞ 处分歧，故集 X 是有限的. 为了定义 X 上的图，我们先来研究 $\mathrm{GL}_2(\mathbf{Q}_p)/\mathrm{GL}_2(\mathbf{Z}_p)\mathcal{Z}(\mathbf{Q}_p)$.

每一个 $\mathrm{GL}_2(\mathbf{Q}_p)$ 中的矩阵

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

都对应了一个秩 2 的 $\mathbf{Z}_p$-模，其基为

$$e_1 = \begin{pmatrix} a \\ c \end{pmatrix}, \quad e_2 = \begin{pmatrix} b \\ d \end{pmatrix}.$$

换句话说，它对应了一个 $\mathbf{Q}_p^2$ 中的格 $L = \mathbf{Z}_p e_1 \bigoplus \mathbf{Z}_p e_2$. 两个 $\mathrm{GL}_2(\mathbf{Q}_p)$ 中的矩阵 g_1, g_2 对应同一个格的充分必要条件是 $g_1^{-1} g_2 \in \mathrm{GL}_2(\mathbf{Z}_p)$. 因此我们可以将 $\mathrm{GL}_2(\mathbf{Q}_p)/\mathrm{GL}_2(\mathbf{Z}_p)$ 视为 $\mathbf{Q}_p^2$ 中的格集. 对两个格 L_1 和 L_2，如果存在非零元 $x \in \mathbf{Q}_p$，使得 $L_1 = xL_2$，则称 L_1, L_2 等价. 因此，$\mathrm{GL}_2(\mathbf{Q}_p)/\mathrm{GL}_2(\mathbf{Z}_p)\mathcal{Z}(\mathbf{Q}_p)$ 参数化 $\mathbf{Q}_p^2$ 中格的等价类集. 将每个等价类视为顶点，两个顶点相邻的充分必要条件是在它们对应的两个格 L_1, L_2 中，L_2 是 L_1 指数为 p 的子格. 如果这样，那么 pL_1 是 L_2 的指数为 p 的子格，因此我们得到了一个无向图. 可以证明

$$g = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

对应顶点的邻点是

$$g = \begin{pmatrix} p & u \\ 0 & 1 \end{pmatrix} \ (0 \leq u \leq p-1) \quad 和 \quad g = \begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix}$$

对应的顶点. 因此 $\mathrm{GL}_2(\mathbf{Q}_p)/\mathrm{GL}_2(\mathbf{Z}_p)\mathcal{Z}(\mathbf{Q}_p)$ 是一个无限 $(p+1)$-正则树，它是任意 $(p+1)$-正则无向图的通用覆盖. 更详细的介绍可

参阅参考文献 [28].

群 $\widetilde{\Gamma}$ 通过左变换作用在 $\mathrm{GL}_2(\mathbf{Q}_p)/\mathrm{GL}_2(\mathbf{Z}_p)\mathcal{Z}(\mathbf{Q}_p)$ 上，其商是一个图，我们记作 X. 由于 $\widetilde{\Gamma}$ 包含了挠元素，故计算重数后， X 是一个 $(p+1)$-正则图.

对 X 上的函数 f, 我们将它视为一个定义在 $D(A_{\mathbf{Q}})$ 上且在 $D(\mathbf{R})$ 左作用及 $\prod\limits_q K_q\mathcal{Z}'(A_{\mathbf{Q}})$ 右作用下不变的自守形式 F. 邻接矩阵 $A(X)$ 在 f 上的作用恰好相当于 Hecke 算子 $\mathbb{T}_p$ 在 F 的作用. 因此， $A(X)$ 的特征值正好是 $\mathbb{T}_p$ 在

$$D(\mathbf{Q})\Big\backslash D(A_{\mathbf{Q}})\Big/D(\mathbf{R})\prod_q K_q\mathcal{Z}'(A_{\mathbf{Q}})$$

上自守形式空间上的特征值. 由于这样的自守形式有平凡的中心特征标，而在

$$D(\mathbf{Q})\Big\backslash D(A_{\mathbf{Q}})\Big/D(\mathbf{R})\prod_q K_q\mathcal{Z}'(A_{\mathbf{Q}})$$

上的自守形式空间可分解为一些子空间的直和，每个子空间是由 $D(A_{\mathbf{Q}})$ 上的一个不可约自守表示 π' 生成. 若 $\pi'=\omega\circ\mathrm{Nrd}$ 是一维的，则 ω 在

$$\mathrm{Nrd}\left(D(\mathbf{R})\prod_q K_q\mathcal{Z}'(A_{\mathbf{Q}})\right)$$

上平凡，后者包含了 $\mathbf{R}_{>0}\cdot\prod\limits_q\mathcal{U}_q$. 由于 $I_{\mathbf{Q}}=\mathbf{Q}^\times\cdot\mathbf{R}_{>0}\cdot\prod\limits_q\mathcal{U}_q$, 所以 ω 是一个平凡特征标，其对应的自守形式空间是一维的，它由 $D(A_{\mathbf{Q}})$ 上的常值函数组成. 这些常值函数都是 $\mathbb{T}_p$ 的特征函数，对应的特征值是 $p+1$. 出现在分解中的剩下表示 π' 是无限维的. 命

$$\pi'=\bigotimes_v{}'\,\pi'_v$$

是这样一个表示. 则 π'_∞ 是 $D(\mathbf{R})$ 的一个平凡表示，而且，按照局部对应，它对应了一个权为 2 的 $\mathrm{GL}_2(\mathbf{R})$ 的离散系列表示 π_∞. 于

是由第八章 §5 定理 16 知，π' 对应的 $\mathrm{GL}_2(A_{\mathbf{Q}})$ 的整体表示

$$\pi = \bigotimes_v' \pi_v$$

是由一个权为 2 的尖点形式 f 诱导出的. $\mathbb{T}_p$ 在位于 π' 的表示空间中的

$$D(\mathbf{Q})\Big\backslash D(A_{\mathbf{Q}})\Big/ D(\mathbf{R})\prod_q K_q \mathcal{Z}'(A_{\mathbf{Q}})$$

上的自守形式上作用的特征值 λ 与 $\mathbb{T}_p$ 在 f 上作用的特征值是相同的. 由被 Deligne 证明了的 Ramanujan–Petersson 猜想 (第七章 §3 定理 6) 知，上述特征值满足

$$|\lambda| \le 2\sqrt{p} = 2\sqrt{k-1}.$$

我们已经证明 $A(X)$ 有一个等于 $k = p+1$ 的特征值，故剩余的特征值的绝对值均 $\le 2\sqrt{k-1}$. 这就证明了下述定理.

定理 8 图 X 是一个 $(p+1)$-正则 Ramanujan 图.

Mestre 和 Oesterlé 在 [22] 中选取 H 为仅在 ∞ 和一个 $\neq p$ 的素数 ℓ 处分歧的四元数代数 H_ℓ, 相应的双陪集空间总是在右边模去实点和在非 Archimedes 位处的标准最大紧子群的积. 然后命 ℓ 趋于无穷，借此构造出 $(p+1)$-正则 Ramanujan 图. 利用这一方法他们得到了无限多个这样的图. 然而， Margulis[20], 及 Lubotzky, Phillips 和 Sarnak[18] (亦可参阅参考文献 [7]) 则取 H 是 Hamilton 四元数，他们通过在 Γ 的同余子群上讨论而得到无穷多个 $(p+1)$-正则 Ramanujan 图. 一般而言，我们既可以通过四元数代数，也可以通过同余子群来构造无限多的 Ramanujan 图. 不过，采用高阶同余子群的一个好处是可以避免重边，即最后得到的商图是真正的 $(q+1)$-正则图.

当基域 $\mathbf{Q}$ 被换成有限域上的单变量函数域时，也有同样的结论成立. 这是因为 Drinfeld[9] 证明了关于函数域上 GL_2 的 Ramanujan 猜想, 从而所得的图一定是 Ramanujan 图. 有关详情可见 Morgenstern 的文章 [23]. 这样构造的图要求 $k = q+1$, 其中 q 是一个

素数的幂. 在参考文献 [27] 中, Pizer 利用经典 Hecke 算子在一些权为 2 的 theta 级数空间上的作用来构造 $(p+1)$-正则 Ramanujan 图, 不过其中需要容许有重边.

§4 由有限交换群构造 Ramanujan 图

在这一节中, 所构造的 Ramanujan 图的顶点是有限交换群中的元素. 我们首先利用交换群来构造 k-正则图. 设 G 是一个有限交换群, S 是 G 的 k-元素集. 利用 S 我们定义两个 k-正则图, 分别称为**和图**$X_s(G,S)$ 和**差图** $X_d(G,S)$. 对 $x\in G$, 它在 $X_s(G,S)$(或 $X_d(G,S)$) 中的外邻点是 G 中那些元素 y, 使得 $x+y\in S$(或 $y-x\in S$), 即 $y\in -x+S$(或 $x+S$). 由定义可以看出, 和图是无向的, 而差图一般来说是有向的; 当且仅当 S 是对称, 即 $S=-S$ 时, 差图是无向的. 这样构造的和图与差图有很好的性质. 对 G 的一个特征标 ψ, 命

$$e(\psi,S)=\sum_{s\in S}\psi(s).$$

命题 1 (1) G 的每个特征标 ψ 均是 $X_d(G,S)$ 的邻接矩阵的特征函数, 对应的特征值是 $e(\psi,S)$.

(2) 若 $e(\psi,S)=0$, 则 ψ 和 ψ^{-1} 均为 $X_s(G,S)$ 的邻接矩阵 $A(X_s)$ 的特征值为 0 的特征函数; 若 $e(\psi,S)\neq 0$, 则

$$|e(\psi,S)|\psi\pm e(\psi,S)\psi^{-1}$$

是 $A(X_s)$ 的两个分别对应特征值为 $\pm|e(\psi,S)|$ 的特征函数.

命题 2 (1) $X_d(G,S)$ 和 $X_s(G,S)$ 的邻接矩阵可被酉矩阵对角化.

(2) $X_d(G,S)$ 和 $X_s(G,S)$ 邻接矩阵的特征值之绝对值是相等的, 均为 $\left|\sum_{s\in S}\psi(s)\right|$, 其中 ψ 跑遍 G 的所有特征标.

习题 2 证明命题 1 和 2.

因此，如果我们能找到一个合适的有限交换群 G 和 G 的一个 k-元素子集 S，使得对 G 的所有的非平凡特征标 ψ，有

$$\left|\sum_{s\in S}\psi(s)\right| \leq 2\sqrt{k-1}.$$

那么 $X_s(G,S)$ 和 $X_d(G,S)$ 一定是 Ramanujan 图．这就把一个组合问题归结为一个特征和估计问题，于是我们可以应用第六章 §3 中所得的特征和估计．

首先回顾一些概念．设 F 是一个有 q 个元素的有限域，F_n 是 F 的次数为 n 的域扩张，N_n 是范映射 $\mathrm{N}_{F_n/F}$ 的核．假定 $n \geq 2$，令 t 为 F_n 中使得 $F_n = F(t)$ 的一个元素．定义集合

$$S_n = \left\{\frac{t^q+a}{t+a} : a \in F\bigcup\{\infty\}\right\}.$$

则 $|S_n| = q+1$．由第六章 §3 定理 6 知，当 $n = 3,4$ 时，$X_s(N_n, S_n)$ 和 $X_d(N_n, S_n)$ 是 Ramanujan 图．事实上，当 $n = 3$ 时，特征和的界是 $\sqrt{q}$，于是我们可以随机地添加 N_3 中的元素来扩大 S，只要添加的元素个数不超过 $\sqrt{q}$ 个，所得到的图仍是 Ramanujan 图．作为第六章定理 7′ 的一个推论，$X_s(F_2, S_2)$ 和 $X_d(F_2, S_2)$ 是 Ramanujan 图．进一步，由第六章定理 9 可知，

$$X_s(N_2 \times F_2, S_2) \text{ 和 } X_d(N_2 \times F_2, S_2)$$

也是 Ramanujan 图．取 $Y = \{t+a : a \in F\}$，由第六章定理 11 导出，$X_s(F_2^\times, Y)$ 和 $X_d(F_2^\times, Y)$ 是 Ramanujan 图，进而取 F 中两个互异的元素 a 和 b，令

$$Y' = \{(a-c, b-c) : c \neq a, b,\ c \in F\}.$$

则 $X_s(F^\times \times F^\times, Y')$ 和 $X_d(F^\times \times F^\times, Y')$ 也是 Ramanujan 图．

最后，我们要说的是，由第六章 §3 所得的特征和的估计可以从 F 上的亏格为 0 的函数域的伊代尔类群的特征标的研究中得到．同样，给出一条在 F 上有 $k \geq q+1$ 个点的椭圆曲线 E，它至少有

一个 F_2-有理点，且该点不是 F-有理点 (当 $q \geq 5$ 时，这一条总是成立的)，那么，我们可以利用 $F_2 \times E(F)$ 来构造 k-正则 Ramanujan 图. 由曲线的 Riemann 猜想知

$$q+1 \leq k \leq q+1+2\sqrt{q}.$$

当 q 是素数时，对一个位于 $q+1$ 和 $q+1+2\sqrt{q}$ 之间的整数 k, 存在一条在 F 上有 k 个点的椭圆曲线. 因此，对每个不小于 5 的素数 p 和 $p+1$ 与 $p+1+2\sqrt{p}$ 之间的整数 k, 总有一个 k-正则 Ramanujan 图，其 p^2k 个顶点可用椭圆曲线构造. 从对小整数 k 的研究我们可以很自然地作出下面的猜测.

猜想 对每个不小于 6 的整数 k, 总存在一个由椭圆曲线构造的 k-正则 Ramanujan 图.

由上面的讨论可知，上述猜想可以用相邻素数的差距来表述. 以 p_n 表第 n 个素数. 则上述猜想等价于:

猜想′ 对充分大的n, $p_{n+1} - p_n \leq 2\sqrt{p_n}$.

有关这一节内容的更详细的情况，读者可以参阅参考文献 [8] 和 [15].

§5 由有限非交换群构造 Ramanujan 图

在这一节里，我们将利用有限非交换群来构造 Ramanujan 图. 不过读者可以从中看到这里仍有许多前两种方法已讨论过的性质. 因此我们先从一般的情形开始.

设 G 是一个有限群，K 是 G 的一个子群. 以 $L(G)$ 表示 G 上的复值函数空间，$L(G/K)$ 表示由在 K 右变换作用下不变的函数组成的子空间. 对一个 K-双边陪集 $S = KsK$, 我们通过把 G 上的函数 f 映为

$$(A_S f)(x) = \sum_{y \in S} f(xy), \quad x \in G$$

来定义一个 $L(G)$ 上的算子 A_S. 设 λ 是 A_K 的一个非 0 的特征值, f 是对应特征值 λ 的特征函数. 在 G 上定义 h_f 为 f 在 K 上的平均

$$h_f(x) = \sum_{k\in K} f(xk), \quad x \in G.$$

则 $h_f \in L(G/K)$ 且

$$f = \left(f - \frac{1}{|K|}h_f\right) + \frac{1}{|K|}h_f,$$

这里 $f - \frac{1}{|K|}h_f$ 位于 A_K 的 0-特征空间 L_0 中.

我们已经证明了

$$L(G) = L(G/K) \bigoplus L_0,$$

其中每个子空间在 G 的左变换下不变. 进一步, A_S 在 L_0 上的作用相当于 0 算子, $L(G/K)$ 是 A_S-不变的.

我们假定所有的算子 A_S 都是可以对角化的, 而且两两交换. 由于 $A_S f$ 就是 f 与 S^{-1} 的特征函数的卷积, 我们的假设导出由 G 上的双边 K-不变函数组成的卷积代数 $L(K\backslash G/K)$ 是交换的. 注意, 如果每个双边陪集 S 都是对称的话, 即 $S = S^{-1}$, 那么我们的假设自然成立. 约定 G 在 $L(G/K)$ 上的左作用为: 对 $g \in G$, 它在 $f \in L(G/K)$ 上的左作用定义为

$$(g\cdot f)(x) = f(g^{-1}x), \quad x \in G.$$

这样 $L(G/K)$ 是算子 A_S 的公共特征空间的直和, 且每个公共特征空间在 G 的左变换作用下不变. 因此 $L(G/K)$ 可分解为 G 的不可约表示 (V,π) 的直和, 且算子 A_S 在每个空间 V 上的作用相当于乘以一个数 λ_S. 我们希望找到一种计算 λ_S 的方法. 记 G 的单位元为 e.

命题 3 *设 (V,π) 是 G 出现于 $L(G/K)$ 中的不可约表示. 则*

(1) 若 h 是 V 中满足 $h(e) = 0$ 的双边 K-不变函数, 则 $h = 0$.

(2) V 中有且只有一个满足 $h(e)=1$ 的双边 K-函数 h.

(3) 对任意的 $x,y\in G$, (2) 中的函数 h 满足

$$\frac{1}{|K|}\sum_{k\in K}h(xky)=h(x)h(y),$$

且对任意的 K-双边陪集 $S=KsK$ 有

$$\lambda_S=\frac{|K|^2}{|\operatorname{Stab}s|}h(s),$$

其中 $\operatorname{Stab}s$ 由使得 $Ksk=Ks$ 的 K 中元素 k 组成.

证 设 f 是 V 中一个非 0 函数, 且存在 $g\in G$ 使得 $f(g)=1$. 必要时将 f 换成 $\pi(g^{-1})f$, 我们总可假定 $f(e)=1$. 定义

$$h(x)=\frac{1}{|K|}\sum_{k\in K}f(kx)=\frac{1}{|K|}\sum_{k\in K}\left(\pi(k)f\right)(x),\quad x\in G.$$

则 $h\in V$, 它是双边 K-不变的, 且满足 $h(e)=f(e)=1$. 这就证明了 (2) 的存在性部分. (2) 的唯一性部分将从 (1) 中得到.

设 h 是 V 中的一个双边 K-不变函数. 则对任意的 K-双边陪集 $S=KsK$, $A_Sh=\lambda_Sh$. 固定 $s\in G$. 对任意的 $x\in G$, 我们有

$$\begin{aligned}\frac{1}{|K|}\sum_{k\in K}h(xks)&=\frac{|\operatorname{Stab}s|}{|K|^2}\sum_{y\in S}h(xy)=\frac{|\operatorname{Stab}s|}{|K|^2}(A_Sh)(x)\\&=\frac{|\operatorname{Stab}s|}{|K|^2}\lambda_Sh(x).\end{aligned}$$

取 $x=e$, 则

$$h(s)=\frac{|\operatorname{Stab}s|}{|K|^2}\lambda_Sh(e).$$

因此对所有的 $s\in G$, 只要 $h(e)=0$, 就有 $h(s)=0$. 这就证明了 (1). 假定 $h(e)=1$, 由上述方程即可导出

$$h(s)=\frac{|\operatorname{Stab}s|}{|K|^2}\lambda_S.$$

于是, 对任意的 $x,y\in G$, 有

$$\frac{1}{|K|}\sum_{k\in K}h(xky)=h(x)h(y),$$

进而 λ_S 即是所需.

注 如果我们在 L_0 中取双边 K-不变函数 h, 则同样的证明导出 $h=0$. 因此 L_0 中没有包含非平凡的双边 K-不变函数. 这就证明了出现在 L_0 中的表示没有 K-不变向量.

上述命题导出, 在 V 中, 由 (2) 中的 h 生成的 $\pi(K)$-不变子空间是一维的. 从而由上面的注可知, 出现于 $L(G/K)$ 中的表示可由 K-不变向量决定. 固定 $x\in G$ 并考虑 V 中的算子

$$\sum_{k\in K}\pi(kx^{-1}):=\rho(x).$$

对 $f\in V$, $\rho(x)f$ 是 V 中的一个双边 K-不变函数, 它在 e 处的值等于

$$\big(\rho(x)f\big)(e)=\sum_{k\in K}f(xke)=|K|f(x).$$

于是, $\rho(x)f=|K|f(x)h$. 取 V 的一组基 $f_1=h,f_2,\cdots,f_r$. $\rho(x)$ 关于这组基的表示矩阵是

$$\begin{pmatrix}|K|h(x) & |K|f_2(x) & |K|f_3(x) & \cdots & |K|f_r(x)\\ 0 & 0 & 0 & & 0\\ \vdots & \vdots & \vdots & & \vdots\\ 0 & 0 & 0 & \cdots & 0\end{pmatrix},$$

从而

$$\frac{1}{|K|}\operatorname{tr}\rho(x)=\frac{1}{|K|}\sum_{k\in K}\operatorname{tr}\pi(kx^{-1})=h(x).$$

总结上述结果我们得到下述定理.

定理 9 *群 G 以左变换的方式作用在 G 的右 K-不变函数空间 $L(G/K)$ 上. 空间 $L(G/K)$ 可分解为一些不可约子空间 (V,π) 的直和, 使得在每个子空间 V 上, 对任意的 K-双边陪集 S, 算子 A_S*

的作用相当于乘以数 $\lambda_{S,\pi}$. 进一步, 在每个不可约子空间 V 中, 左 K-不变函数空间是一维的, 它由

$$h_\pi(x) := \frac{1}{|K|}\sum_{k\in K} \operatorname{tr}\pi(kx^{-1}) \tag{5.1}$$

生成. 这样的函数是双边 K-不变的, 它满足 $h_\pi(e)=1$, 且对任意的 $x,y\in G$, 有

$$\frac{1}{|K|}\sum_{k\in K} h_\pi(xky) = h_\pi(x)h_\pi(y).$$

因此, 特征值 $\lambda_{S,\pi}$ 可由下式得到

$$\lambda_{S,\pi} = \frac{|K|^2}{|\operatorname{Stab} s|}h_\pi(s), \quad s\in S,$$

其中 $\operatorname{Stab} s$ 是由使得 $Ksk=Ks$ 的 $k\in K$ 组成.

现在我们开始图的构造. 设 T 是有限个 K-双边陪集的并. 在陪集 G/K 上定义 Cayley 图 $X=\operatorname{Cay}(G/K,T/K)$: 设

$$T=\bigcup_{i=1}^{k} g_iK$$

是 K-陪集的不交并, 定义 xK 的外邻点 (即以 xK 为起点的邻点. 提醒一下, 我们所考虑的图是有向图) 为 xg_iK, $i=1,\cdots,k$. 这是一个 k-正则有向图, 且当 $T=T^{-1}$ 时, 它是无向的. 若 G 是交换的且 K 由单位元组成, 则这恰好是上一节定义的差图. 当

$$G=\mathrm{PGL}_2(\mathbf{Q}_p), \quad K=\mathrm{PGL}_2(\mathbf{Z}_p), \quad T=K\begin{pmatrix} p & 0\\ 0 & 1\end{pmatrix}K$$

时, 所得的图则是 §2 中结合 $\mathrm{PGL}_2(\mathbf{Q}_p)$ 的 $(p+1)$-正则的无限树 $\mathcal{T}$.

Cayley 图 $X=\operatorname{Cay}(G/K,T/K)$ 的邻接矩阵 $\overline{A}_T$ 是 $\frac{1}{|K|}\sum_{S\subset T} A_S$. 利用上述定理知, $\overline{A}_T$ 的特征值由

$$\sum_{S\subset T}\frac{|K|}{|\operatorname{Stab} s|}h_\pi(s) \quad (s \text{ 为} S \text{ 中任一元素})$$

给出，其中 π 取遍 G 的所有出现在 $L(G/K)$ 中的全部不可约表示.

由前面的评注可知， G 的一个不可约表示 π 出现在 $L(G/K)$ 中的充分必要条件是它有一个非 0 的 K-不变向量. 因此如果采用上述方法构造 Ramanujan 图，那么我们只需要找到合适的 G, K 和 T, 使得 $L(K\backslash G/K)$ 是一个交换代数；对任意的 K-双边陪集 S, A_S 可对角化；对 G 的每个包含了非零 K-不变向量的非平凡不可约表示 π, 由 (5.1) 式定义的函数 h_π 满足

$$\left|\sum_{S\subset T}\frac{|K|}{|\operatorname{Stab} s|}h_\pi(s)\right|\leq 2\sqrt{k-1},$$

其中

$$k=\sum_{S\subset T}\frac{|K|}{|\operatorname{Stab} s|},\quad s\in S.$$

有一类 $(q+1)$-正则 Ramanujan 图是由 Terras 和她的学生构造和研究的 (参阅参考文献 [2], [5]，以及它们所附的参考文献). 他们取定一个有 q 个元素的有限域 F, 其中 q 是个奇数. 命 $G=\mathrm{GL}_2(F)$. 在 F 中选取一个非平方元素 δ, 则 $E=F(\sqrt{\delta})$ 为 F 的二次域扩张. 把 F 上乘以 $x\in E^\times$ 的运算用关于基 $\{1,\sqrt{\delta}\}$ 的矩阵来表示，从而将 $E^\times=F(\sqrt{\delta})^\times$ 嵌入到 G 中. 记嵌入的像为

$$K=\left\{\begin{pmatrix}a & b\delta\\ b & a\end{pmatrix}\in G:a,b\in F\right\}.$$

陪集空间 G/K 的代表可取为

$$H=\left\{\begin{pmatrix}y & x\\ 0 & 1\end{pmatrix}:y\in F^\times,\quad x\in F\right\}.$$

于是它可以模拟经典的 Poincaré 上半平面. 群 G 有 q 个双边陪集，其中

$$K\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}K=K,\quad K\begin{pmatrix}-1 & 0\\ 0 & 1\end{pmatrix}K=\begin{pmatrix}-1 & 0\\ 0 & 1\end{pmatrix}K,$$

剩余的 $q-2$ 个双边陪集 KtK 是 $(q+1)$ 个 K-陪集的并. 更精确一些, 每个双边陪集 KtK 结合了一个椭圆 $x^2=ay+\delta(y-1)^2$, 其中 $a\in F$, $a\neq 0,4\delta$, 使得

$$KtK=\bigcup\begin{pmatrix} y & x\\ 0 & 1\end{pmatrix}K,$$

这里 (x,y) 取遍椭圆上的 F-点. 用 S_a 表示双边陪集 KtK. 取 $T=S_a$, $a\neq 0,4\delta$, 我们得到一个 $(q+1)$-正则 Cayley 图

$$X=\mathrm{Cay}(G/K,\ T/K).$$

由于所有的 K-双边陪集 S 都是对称的, 即 $S=S^{-1}$, 于是图 $X=\mathrm{Cay}(G/K,\ T/K)$ 是无向的且代数 $L(K\backslash G/K)$ 是交换的. 进而, $\mathrm{Stab}\,t$ 是 K 中的对角矩阵子群, 因此

$$|\,\mathrm{Stab}\,t|=q-1,\quad |K|/|\,\mathrm{Stab}\,t|=q+1=k.$$

我们可以从参考文献 [26] 中列出的有关 G 的表示的表中看出, 有两种类型的 G 的不可约非平凡表示包含一个非 0 的 K-不变向量. 第一种是由

$$\begin{pmatrix} a & b\\ 0 & d\end{pmatrix}\longmapsto \chi(a)\chi(d)$$

给出的 Borel 子群的一维表示所诱导的 G 上的 $q+1$ 维表示, 其中 χ 是 $F^{\times}$ 的特征标. 若 χ 的阶大于 2, 则上述的诱导表示是不可约的, 记作 π_χ; 若 χ 的阶为 2, 则用 π_χ 表示上述诱导表示的 q 维不可约子表示. π_χ 在 $L(G/K)$ 中的实现是由 G/K 上的函数 f 的左变换生成的子空间, 其中 f 的左变换定义为

$$f\left(\begin{pmatrix} y & x\\ 0 & 1\end{pmatrix}K\right)=\chi(y).$$

(诱导表示的其他组成部分是一维的, 它们可在 L_0 中实现.)

容易看出, $\overline{A}_T$ 在 π_χ 的表示空间中的特征值 $\lambda_{T,\chi}$ 满足下面

关系式

$$\lambda_{T,\chi} = \sum_{\substack{y \in F \\ ay+\delta(y-1)^2=x^2}} \chi(y).$$

R. Evans 和 H. Stark 利用 Weil[34] 关于 F 上射影曲线的 Riemann 猜想的结果证明了，当 χ 是非平凡时，

$$\left|\lambda_{T,\chi}\right| \leq 2\sqrt{q} = 2\sqrt{k-1}.$$

Soto Andrade[30] 在 (5.1) 式中取 $\pi = \pi_\chi$, 借此算出了 h_χ, 并由此得到了 $\lambda_{T,\chi}$ 的同样的表达形式. 由于 $T = T^{-1}$, 所以对所有出现在 $L(G/K)$ 中的表示 π, 我们有

$$\lambda_{T,\pi} = \frac{|K|}{q-1} h_\pi(t^{-1}) = \frac{1}{q-1} \sum_{k \in K} \operatorname{tr} \pi(kt).$$

第二种类型 G 的不可约表示结合了一个 F 二次域扩张 $F(\sqrt{\delta})$ 的乘法特征标 ω, 我们记作 π_ω. 注意，这里要求 $\omega \neq \omega^q$, 即 ω 在从 $F(\sqrt{\delta})$ 到 F 的范映射的核上是非平凡的. $\overline{A}_T$ 在 π_ω 的表示空间上的特征值 $\lambda_{T,\omega}$ 是由 Soto-Andrade[30] 算出的:

$$\lambda_{T,\omega} = \sum_{\substack{z=x+y\sqrt{\delta} \in F(\sqrt{\delta}) \\ x^2-\delta y^2=1}} \varepsilon\left(\frac{a}{\delta} - 2 + 2x\right) \omega(z),$$

其中

$$\varepsilon(x) = \begin{cases} 1, & \text{若 } x \text{ 是 } F^\times \text{ 中平方元素;} \\ -1, & \text{若 } x \text{ 不是 } F^\times \text{ 中平方元素;} \\ 0, & \text{若 } x = 0. \end{cases}$$

利用平展上同调理论与代数几何， N. Katz[14] 证明了

$$\left|\lambda_{T,\omega}\right| \leq 2\sqrt{q} = 2\sqrt{k-1}.$$

事实上，上述不等式可以直接从 Weil 的结果中得出. 在下面定理中，我们将利用第六章的知识给出 $\lambda_{T,\chi}$ 和 $\lambda_{T,\omega}$ 的估计.

定理 10 设 δ 是有 q 个元素的有限域 F 中的非平方元素，其中 q 是个奇数，$a \in F$，且 $a \neq 0, 4\delta$. 设 χ 是 $F^{\times}$ 的非平凡特征标，ω 是 F 的二次扩域 $K(\sqrt{\delta})$ 的乘法特征标，且 $\omega \neq \omega^{q}$. 同前一样，假设

$$\lambda_{T,\chi} = \sum_{\substack{y \in F \\ ay+\delta(y-1)^2=x^2}} \chi(y)$$

和

$$\lambda_{T,\omega} = \sum_{\substack{z=x+y\sqrt{\delta}\in F(\sqrt{\delta}) \\ x^2-\delta y^2=1}} \varepsilon\left(\frac{a}{\delta} - 2 + 2x\right)\omega(z),$$

其中

$$\varepsilon(x) = \begin{cases} 1, & \text{若 } x \text{ 是 } F^{\times} \text{ 中平方元素;} \\ -1, & \text{若 } x \text{ 不是 } F^{\times} \text{ 中平方元素;} \\ 0, & \text{若 } x = 0. \end{cases}$$

则

$$\left|\lambda_{T,\chi}\right| \leq 2\sqrt{q}, \quad \text{和} \quad \left|\lambda_{T,\omega}\right| \leq 2\sqrt{q}.$$

证 设 $f(y) = \delta(y-1)^2 + ay$. 首先假定 f 在 F 上不可约. 用 w 表示由 $f(y)$ 的根确定的二次位. 利用第六章 §2 定理 4, 存在一个 $F(t)$ 的伊代尔类特征标 η, 使得在一个具有局部单值化元素

$$\varpi_v = P_v(t) = \prod_{j=1}^{\deg v} (t - \beta_{j,v})$$

的有限位 $v \neq w$ 处有

$$\eta_v(\varpi_v) = \varepsilon\left(\prod_{j=1}^{\deg v} f(\beta_{j,v})\right), \quad \eta_v(\mathcal{U}_v) = 1,$$

而在位 $v = w$ 或 ∞ 处，η_v 在 $1 + \mathfrak{p}_v$ 上平凡. 进一步，η 的前导子是 $w + \infty$. 另一方面，存在一个具有前导子 $0 + \infty$ 的 $F(t)$ 的伊代

尔类特征标 ξ, 使得 ξ_0 在 $\mathcal{U}_0/(1+\mathfrak{p}_0)$ 上由 $\xi_0(a)=\chi^{-1}(a)$ $(a\in F^\times)$ 给出, 而 ξ_∞ 在 $\mathcal{U}_\infty/(1+\mathfrak{p}_\infty)$ 上由 $\xi_\infty(a)=\chi(a)$ $(a\in F^\times)$ 给出, 并且 $\xi_\infty(t^{-1})=\xi_\infty(\varpi_\infty)=1$. 于是 $\xi\eta$ 是有理函数域 $F(t)$ 的一个具有前导子 $w+0+\infty$ 或 $w+0$ 的次数为 4 或 3 的特征标. 在一个次数为 1 且 $\varpi_v=t-\beta$ 的有限位 v 处, 其中 ξ 和 η 是非分歧的, 我们有

$$\xi_v(\varpi_v)=\xi_\infty(t-\beta)^{-1}\xi_0(t-\beta)^{-1}=\chi(-\beta)$$

和

$$\eta_v(\varpi_v)=\varepsilon\big(f(\beta)\big).$$

当 $\eta\xi$ 的前导子是 $w+0+\infty$ 时, 由第六章 §1 推论 2 得

$$\left|\sum_{\substack{v\neq 0,\infty\\ \deg v=1}}\eta_v\xi_v(\varpi_v)\right|=\left|\sum_{y\in F^\times}\chi(-y)\varepsilon\big(f(y)\big)\right|=\left|\sum_{y\in F}\chi(y)\varepsilon\big(f(y)\big)\right|$$
$$\leq 2\sqrt{q}.$$

当 $\eta\xi$ 的前导子是 $w+0$ 时, 同样有

$$\left|\eta_\infty\xi_\infty(\varpi_\infty)+\sum_{y\in F^\times}\chi(-y)\varepsilon\big(f(y)\big)\right|\leq\sqrt{q}.$$

由此得出同样的界

$$\left|\sum_{y\in F}\chi(y)\varepsilon\big(f(y)\big)\right|\leq\sqrt{q}+1\leq 2\sqrt{q}.$$

由于 χ 是非平凡的, 于是 $\sum\limits_{y\in F}\chi(y)=0$, 因此

$$\sum_{y\in F}\chi(y)\varepsilon\big(f(y)\big)=\sum_{y\in F}\chi(y)\varepsilon\big(f(y)\big)+\sum_{y\in F}\chi(y)=2\lambda_{T,\chi}.$$

由此再结合上述不等式即得 $|\lambda_{T,\chi}|\leq\sqrt{q}$.

若 f 在 F 上可约, 则由 $a\neq 0,4\delta$ 可知它有两个互异的根. 记 v_1,v_2 为对应这两个根的 F 的两个次数为 1 的位. 由于 $\delta\neq 0$, 从

而 $v_1, v_2 \neq 0$. 我们可以同前一样定义一个前导子为 $v_1 + v_2 + \infty$ 的特征标 η, 于是 $\xi\eta$ 的前导子是 $0 + v_1 + v_2 + \infty$ 或 $0 + v_1 + v_2$. 同样由第六章 §1 推论 2 可得, 无论何种情形, 我们有

$$\left|\sum_{y \in F} \chi(y)\varepsilon\big(f(y)\big)\right| \leq 2\sqrt{q}.$$

又由于

$$\begin{aligned}\sum_{y \in F} \chi(y)\varepsilon\big(f(y)\big) &= \sum_{y \in F} \chi(y)\varepsilon\big(f(y)\big) + \sum_{y \in F} \chi(y) \\ &= 2\lambda_{T,\chi} - \chi(v_1) - \chi(v_2),\end{aligned}$$

由此即得 $\left|\lambda_{T,\chi}\right| \leq \sqrt{q} + 1 \leq 2\sqrt{q}$.

最后, 我们来估计 $\lambda_{T,\omega}$. 用 w 表示 $F(t)$ 的一个次数为 2 的位, 其对应的局部单值化元素是 $\varpi_w = t^2 - \delta$. 在 w 的剩余类域 $F(\sqrt{\delta})$ 中范数为 1 的元素均可写成

$$z = \frac{-\sqrt{\delta} - b}{\sqrt{\delta} - b} = \frac{b^2 + \delta + 2b\sqrt{\delta}}{b^2 - \delta},$$

其中 $b \in F \bigcup \{\infty\}$ (当 $b = \infty$ 时, 取 $z = 1$). 于是我们可以将 $\lambda_{T,\omega}$ 展开为

$$\begin{aligned}\lambda_{T,\omega} &= \sum_{b \in F \cup \{\infty\}} \varepsilon\left(\frac{a}{\delta} - 2 + 2\frac{b^2 + \delta}{b^2 - \delta}\right)\omega\left(\frac{-\sqrt{\delta} - b}{\sqrt{\delta} - b}\right) \\ &= \sum_{b \in \mathbf{P}^1(F)} \varepsilon\big(f(b)\big)\omega\left(\frac{-\sqrt{\delta} - b}{\sqrt{\delta} - b}\right),\end{aligned}$$

其中

$$f(t) = \frac{f_1(t)}{f_2(t)}, \quad f_1(t) = \frac{a}{\delta}t^2 - a + 4\delta, \quad f_2(t) = t^2 - \delta.$$

由第六章 §3 定理 6 的证明可知, 存在 $F(t)$ 的一个伊代尔类特征标 ξ, 它在 $\neq w$ 的位上非分歧, 而 ξ_w 在 $F^\times(1 + \mathfrak{p}_w)$ 上平凡, 在

$\xi_w/F^\times(1+\mathfrak{p}_w)$ 上则由

$$\xi_w(\alpha+\beta t)=\omega\left(\frac{\alpha+\beta\sqrt{\delta}}{\alpha-\beta\sqrt{\delta}}\right)$$

给出，其中 $\alpha,\beta\in F,\alpha+\beta t\in\mathcal{U}_w$. 此外 ξ_∞ 还是平凡的. 由于 ω 在 $F(\sqrt{\delta})$ 中范数为 1 的元素上非平凡，故 ξ 的前导子是 w. 在 $F(t)$ 的任意次数为 1, 且 $\varpi_v=t-b$ 或 $v=\infty,\varpi_\infty=1/t$ 的位 v 处，我们有

$$\xi_v(\varpi_v)=\omega\left(\frac{-\sqrt{\delta}-b}{\sqrt{\delta}-b}\right),$$

其中当 $v=\infty$ 时，$b=\infty$. 回忆支集的定义：f 的支集是 $F(t)$ 的所有使得 f 有零点或极点的位的并. 对于上述的 $f(t)=f_1(t)/f_2(t)$, 由于 $a\neq 4\delta$, 故 $f_1(t)$ 没有重根. 因此

$$\operatorname{supp} f=\{w_1,w\}\text{ 或 }\{v_1,v_2,w\},$$

其中，若 $f_1(t)$ 是不可约的，则 w_1 是 $F(t)$ 的一个由 $f_1(t)$ 的根决定的次数为 2 的位；若 $f_1(t)$ 是可约的，则 v_1,v_2 是 $F(t)$ 的对应于 $f_1(t)$ 的两个不同的根的次数为 1 的位. 在 $F(t)$ 的不在 $\operatorname{supp} f$ 中的位 v 处，像前面一样定义特征标 η_v, 又定义

$$\eta_\infty(\varpi_\infty)=\varepsilon\big(f(\infty)\big)=\varepsilon(a\delta^{-1}),\quad \eta_\infty(\mathcal{U}_\infty)=1,$$

将此扩充为 $F(t)$ 的一个伊代类特征标 η, 其前导子为

$$\operatorname{cond}\eta=\sum_{v\in\operatorname{supp} f}v.$$

因此，$\eta\xi$ 的前导子的次数是 2 或 4, 从而由第六章 §1 推论 2 得

$$\left|\sum_{\substack{\deg v=1\\ \eta_v\xi_v\text{ 非分歧}}}\eta_v(\varpi_v)\xi_v(\varpi_v)\right|=\left|\sum_{b\in\mathbf{P}^1(F)}\varepsilon\big(f(b)\big)\omega\left(\frac{-\sqrt{\delta}-b}{\sqrt{\delta}-b}\right)\right|$$

$$=\left|\lambda_{T,\omega}\right|\le 2\sqrt{q}.$$

这就完成了定理 10 的证明.

定理 11 图 $X = \mathrm{Cay}(G/K,\ S_a/K)$, $a \in F$, $a \neq 0, 4\delta$, 是 $(q+1)$-正则 Ramanujan 图.

这是 Ramanujan 图的第三种构造方法, 它既用到了有限域上 GL_2 的表示, 又用到了由有限域上曲线的 Riemann 猜想所得的特征和的估计. 欲知更详细的材料, 读者可以参阅参考文献 [2], [5], [10], [16] 和 [17].

§6 Alon-Boppana 定理的两个证明

在这一节中, 我们将给把定理 7 视为两个不同的定理的推论而给出它的两种不同的证明. 需要说明的是, 这一节的结果对更一般的超图也成立, 这个推广是由冯克勤、李文卿[11] 完成的.

我们回到定理 7 的证明上来, 第一种方法是源于 Nilli 的关于图 G 的直径与 G 的第二大特征值 $\lambda_2(G)$ 之间关系的工作. 注意 $\lambda(G) \geq \lambda_2(G)$.

定理 12[24] 设 G 是一个 k-正则图, 记 $k-1$ 为 q. 若 G 的直径 $\geq 2l+2 \geq 4$, 则

$$\lambda_2(G) > 2\sqrt{q} - \frac{2\sqrt{q}-1}{l}.$$

记 D 为图 G 的直径. 则

$$|G| \leq 1 + k + k \cdot q + \cdots + k \cdot q^{D-1} < 1 + k + \cdots + k^D.$$

由此导出

$$D \geq \frac{\log |V(G)|}{\log k} - O(1),$$

其中 $V(G)$ 表示 G 的顶点集. 因此当 $|G| \to \infty$ 时, G 的直径也趋于无穷. 从而容易地看出, 当 $|G| \to \infty$ 时, $\liminf \lambda_2(G)$ 至少是 $2\sqrt{q}$, 进而

$$\liminf \lambda(G) \geq 2\sqrt{q}.$$

证 不失一般性，假定 G 是连通的. 将邻接矩阵 A 视为 G 的顶点集上实值函数空间 $\mathcal{F}(G)$ 上的一个线性算子

$$A: f \longmapsto Af,$$
$$(Af)(x) = \sum_{y} f(y),$$

其中 y 跑遍 G 中 x 的所有邻点. 设 Δ 是 $\mathcal{F}(G)$ 上的 Laplace 算子 $kI - A$, 则在 $\mathcal{F}(G)$ 上有一个自然的内积 $\langle\ ,\ \rangle$:

$$\langle f_1, f_2 \rangle = \sum_{x \in V(G)} f_1(x)\, f_2(x).$$

$\mathcal{F}(G)$ 有一组均为 Δ 的特征函数的正交基. 显然，常值函数 $f_0 \equiv 1$ 是一个特征值为 0 的特征函数， Δ 的其他特征值都是正的，它们对应的特征函数与常值函数 f_0 垂直. Δ 的第二小的特征值 α 是 $k - \lambda_2(G)$, 它也等于

$$\alpha = \min_{\substack{f \neq 0,\ f \in \mathcal{F}(G) \\ \langle f, f_0 \rangle = 0}} \frac{\langle \Delta f, f \rangle}{\langle f, f \rangle}.$$

我们将通过特别选取 f 来给出 α 的上界.

由假定， G 的直径 $\geq 2l + 2 \geq 4$, 于是我们可找到 G 的两个顶点 u 和 v, 它们之间的距离 $\operatorname{dist}(u, v) \geq 2l + 2$. 对 $i \geq 0$ 定义

$$U_i = \{x \in V(G) \operatorname{dist}(x, u) = i \text{ 的顶点}\}$$

和

$$V_i = \{x \in V(G) \operatorname{dist}(x, v) = i \text{ 的顶点}\}.$$

则 $U_0, \cdots, U_l, V_0, \cdots, V_l$ 是互不相交的，并且

$$U = \bigcup_{i=0}^{l} U_i$$

中的顶点与

$$V = \bigcup_{i=0}^{l} V_i$$

中顶点都不相邻. 定义一个 G 上的函数 f 为

$$f(x) = \begin{cases} a, & \text{若 } x \in U_0 \bigcup U_1, \\ a\,q^{-(i-1)/2}, & \text{若 } x \in U_i, \quad 2 \le i \le l, \\ -b, & \text{若 } x \in V_0 \bigcup V_1, \\ -b\,q^{-(i-1)/2}, & \text{若 } x \in V_i, \quad 2 \le i \le l, \\ 0, & \text{其他}, \end{cases}$$

这里 a, b 是任意两个使得 f 垂直于 f_0 的正数.

首先我们来估计

$$\langle f, f\rangle = \sum_{x\in U} f(x)^2 + \sum_{x\in V} f(x)^2.$$

显然, $|U_0| = 1$, $|U_1| = k$. 对每个顶点 $x \in U_i (i \ge 1)$, 在它的 k 个邻点中, 至少有一个点位于 U_{i-1} 中, 且至多有 $q = k - 1$ 个点在 U_{i+1} 中. 这就证明了, 当 $i = 1, \cdots, l-1$ 时, $|U_{i+1}| \le q|U_i|$. 因此

$$\begin{aligned} A_1 &= \sum_{x\in U} f(x)^2 = a^2\left(1 + |U_1| + \sum_{i=2}^{l} |U_i|\, q^{-(i-1)}\right) \\ &\ge a^2\left(1 + l\,\frac{|U_l|}{q^{l-1}}\right). \end{aligned} \tag{6.1}$$

类似地,

$$B_1 = \sum_{x\in V} f(x)^2 \ge b^2\left(1 + l\,\frac{|V_l|}{q^{l-1}}\right).$$

接下来估计 $\langle \Delta f, f\rangle$. 以 $E(G)$ 表示 G 的边集合. 容易看出

$$\begin{aligned} \sum_{\{x,y\}\in E(G)} \big(f(x) - f(y)\big)^2 &= \sum_{\{x,y\}\in E(G)} f(x)^2 - 2f(x)f(y) + f(y)^2 \\ &= k\sum_{x\in G} f(x)^2 - \sum_{x\in G} f(x) \sum_{\substack{y\in G \\ \{y,x\}\in E(G)}} f(y) \\ &= k\langle f, f\rangle - \langle Af, f\rangle = \langle \Delta f, f\rangle. \end{aligned}$$

命 $\langle \Delta f, f\rangle = A_2 + B_2$, 其中

$$A_2 = \sum_{\substack{\{x,y\}\in E(G)\\ x,y\text{ 中至少有一个在 } U \text{ 中}}} \big(f(x)-f(y)\big)^2,$$

$$B_2 = \sum_{\substack{\{x,y\}\in E(G)\\ x,y\text{ 中至少有一个在 } V \text{ 中}}} \big(f(x)-f(y)\big)^2.$$

从 f 的定义以及 $x \in U_i$ 在 U_{i+1} 中至多有 q 个邻点可知

$$\begin{aligned}
A_2 &\le \sum_{i=1}^{l-1} |U_i| q\left(q^{-\frac{i-1}{2}} - q^{-\frac{i}{2}}\right)^2 a^2 + |U_l| q\cdot q^{-(l-1)}a^2\\
&= (\sqrt{q}-1)^2\left(|U_1| + |U_2|q^{-1} + \cdots + |U_l|q^{-(l-1)}\right)a^2\\
&\quad + a^2(2\sqrt{q}-1)|U_l|q^{-(l-1)}\\
&\le (\sqrt{q}-1)^2(A_1-a^2) + (2\sqrt{q}-1)\cdot\frac{A_1-a^2}{l}\ (\text{利用 (6.1)})\\
&< \left(1+q-2\sqrt{q}+\frac{2\sqrt{q}-1}{l}\right)A_1.
\end{aligned}$$

类似地，我们有

$$B_2 < \left(1+q-2\sqrt{q}+\frac{2\sqrt{q}-1}{l}\right)B_1.$$

因此

$$k-\lambda_2(G) = \alpha \le \frac{A_2+B_2}{A_1+B_1} < 1+q-2\sqrt{q}+\frac{2\sqrt{q}-1}{l},$$

由此导出

$$\lambda_2(G) > 2\sqrt{q} - \frac{2\sqrt{q}-1}{l}.$$

这就完成了定理 12 的证明.

第二种证明 Alon-Boppana 定理的方法是由下面这个描述正则图的大特征值分布的定理而得. 这一定理是 Serre[29] 给出的, 在参考文献 [18] 中也可找到.

定理 13 对任意的 $\varepsilon > 0$, 存在一个仅依赖于 ε 和 k 的正常数 c, 使得对所有的 k-正则图 G, 其满足

$$\lambda \geq (2-\varepsilon)\sqrt{k-1}$$

的特征值 λ 的数目至少是 $c|G|$.

在证明这个定理之前，我们先引入一个与 k-正则图 G 相关的测度 μ_G, 并且讨论它的一些在后面证明中将用到的性质. 以 q 表 $k-1$. 设 $M = k/\sqrt{q}$. 测度 μ_G 在区间 $[-M, M]$ 上的定义是

$$\mu_G = \frac{1}{|G|}\sum_{\lambda} \delta_{\lambda/\sqrt{q}},$$

其中 λ 跑遍 G 的所有特征值；在区间 $[-M, M]$ 外，μ_G 定义为 0. 换句话说，μ_G 的支集包含于 $[-M, M]$. 我们知道，实直线上的测度是由它在多项式族 $\{X_n(x) : \deg X_n = n\}$ 上的取值所决定的. 为方便起见，我们如下选取

$$X_n(x) : X_0(x) = 1, \quad X_1(x) = x,$$

当 $i \geq 2$ 时，我们用递推公式

$$X_i(x) = xX_{i-2}(x) - X_{i-1}(x)$$

来定义 $X_i(x)$. 事实上，这些多项式都是熟知的，如 $X_m(2x)$ 就是第二类 Chebychev 多项式. 我们把 $X_m(x)$ 的一些将要用到的性质列举如下.

(I) 作为 t 的一个形式幂级数，我们有

$$\sum_{m=0}^{\infty} X_m(x)t^m = \frac{1}{1-xt+t^2}.$$

(II) $X_m(x) = \prod_{j=1}^{m}\left(x - 2\cos\frac{j\pi}{m+1}\right)$.

因此每个 X_m 在区间 $(-2, 2)$ 中至少有 m 个不同的实根，且当 m 趋于无穷时，$X_m(x)$ 的最大根趋于 2.

(III) $\{X_m(x)\}$ 关于区间 $[-2,2]$ 上由

$$\rho(x)=\frac{1}{\pi}\sqrt{1-\frac{x^2}{4}}\,\mathrm{d}x$$

定义的 Sato-Tate 测度 $\rho(x)$ 是正交的，即

$$\int_{-2}^{2} X_i(x)\,X_j(x)\,\rho(x)=\delta_{ij}.$$

设 $a=\dfrac{1}{\sqrt{q}}$. 我们定义一类新的多项式： $Y_0(x)=1$, 当 $i\geq 1$ 时，

$$Y_i(x)=X_i(x)+aX_{i-1}(x).$$

利用 $X_m(x)$ 递推公式可得性质 (IV)：

(IV) $\{Y_m(x)\}_{m\geq 0}$ 满足 t 的一个形式幂级数关系

$$\sum_{m=0}^{\infty} Y_m(x)\,t^m=\frac{1+at}{1-xt+t^2}.$$

进一步，利用归纳法可以证明下述性质 (V)：

(V) $Y_i(x)\,Y_j(x)=\big(Y_{i+j}(x)+Y_{i+j-2}(x)+\cdots\big)+a\big(Y_{i+j-1}(x)+Y_{i+j-3}(x)+\cdots\big)$.

由 (II) 和 $Y_m(x)$ 的定义可得性质 (VI)：

(VI) $\deg Y_m(x)=m$, 且 $Y_m(x)$ 有 m 个不同的实根，其中最大的实根 α_m 位于

$$2\cos\frac{\pi}{m}\ \ 和\ \ 2\cos\frac{\pi}{m+1}$$

之间. 因此 $\alpha_m\in(-2,2)$ 且 α_m 在 m 趋于无穷时趋于 2.

为求值 $\mu_G(Y_m)$, 我们考虑 G 的函数空间 $\mathcal{F}(G)$ 上的两个算子类. 对 $l\geq 0$, 在 $\mathcal{F}(G)$ 上利用将 f 映为

$$(U_l f)(x)=\sum_p f(y(p))$$

来定义算子 $U_l = U_l(G)$, 其中 p 跑遍 G 中所有由 x 为起点, 长度为 l, 且不折反的 (有向) 路径, $y(p)$ 表示路径 p 的终点. 则 $U_0 = I(=$ 单位元),

$$U_1 = A(G) := A, \quad U_2 = U_1 A - kI,$$

且在 $i \geq 3$ 时,

$$U_i = U_{i-1}A - qU_{i-2}.$$

这可以用形式幂级数来表示

$$\sum_{m=0}^{\infty} U_m t^m = \frac{(1-t)(1+t)}{1 - At + qt^2}.$$

利用

$$\sum_{m=0}^{\infty} T_m t^m = \frac{1+t}{1 - At + qt^2}, \tag{6.2}$$

我们定义 $\mathcal{F}(G)$ 的另一个算子类 $\{T_m\}_{m\geq 0}$. 换句话说,

$$T_m = U_m + U_{m-1} + \cdots + U_1 + U_0.$$

比较 (IV) 和 (6.2) 式可得

$$q^{-m/2} T_m = Y_m\left(\frac{A}{\sqrt{q}}\right), \quad m \geq 0. \tag{6.3}$$

由于 A 可被对角化以及算子的迹在共扼运算下不变, 于是从 μ_G 的定义及 (6.3) 式得

$$\mu_G(Y_m) = \frac{1}{|G|}\sum_{\lambda} Y_m = \frac{1}{|G|} q^{-m/2}\mathrm{Tr}\,(T_m), \quad m \geq 0. \tag{6.4}$$

这是我们研究的关键. 进一步, 利用取每个顶点的特征函数作为 $\mathcal{F}(G)$ 的基, 我们立即看到算子 U_m 的迹是非负的, 从而 T_m 的迹也是非负的. 结合 (6.4) 式, 这就导出, 对任意的 $m \geq 0$,

$$\mu_G(Y_m) \geq 0. \tag{6.5}$$

现在我们来证明定理 13. 证明的关键是找到一个 $Y_m(x)$ 的非负线性组合，且使得其值是可控制的. 为此，我们首先证明下面的命题.

命题 4 记 α_m 为 $Y_m(x)$ 的最大实根. 设

$$Z_m(x) = \frac{Y_m(x)^2}{x - \alpha_m}.$$

则

$$Z_m(x) = \sum_{j=0}^{2m-1} y_j Y_j(x),$$

其中 $y_0 = 0$, 且当 $0 \le i < [m/2]$ 时，有

$$y_{2m-(2i+1)} = y_{2i+1} = Y_0(\alpha_m) + Y_2(\alpha_m) + \cdots + Y_{2i}(\alpha_m) > 0,$$

$$y_{2m-(2i+2)} = y_{2i+2} = Y_1(\alpha_m) + Y_3(\alpha_m) + \cdots + Y_{2i+1}(\alpha_m) > 0.$$

证 显然 $Z_m(x)$ 是一个次数为 $2m-1$ 的多项式，因此它是 $Y_0(x), \cdots, Y_{2m-1}(x)$ 的一个线性组合，记该线性组合的系数为 $y_0, \cdots, y_{2m-1}$. 现在的问题是证明 y_i 恰好是上面所描述的系数. 由于当 $j \ge 1$ 时有 $xY_j(x) = Y_{j+1}(x) + Y_{j-1}(x)$, 同时利用 (V) 可知

$$\begin{aligned} Y_m^2(x) = &(Y_{2m}(x) + Y_{2m-2}(x) + \cdots + Y_2(x) + Y_0(x)) \\ &+ a\,(Y_{2m-1}(x) + Y_{2m-3}(x) + \cdots + Y_3(x) + Y_1(x)). \end{aligned}$$

于是我们有

$$\begin{aligned} Y_m(x)^2 &= (x - \alpha_m) Z_m(x) = (x - \alpha_m) \sum_{j=0}^{2m-1} y_j Y_j(x) \\ &= y_0\big(xY_0(x) - \alpha_m\big) + \sum_{j=1}^{2m-1} y_j \big(xY_j(x) - \alpha_m Y_j(x)\big) \\ &= y_0\big(Y_1(x) - a - \alpha_m\big) \\ &\quad + \sum_{j=1}^{2m-1} y_j \big(Y_{j+1}(x) + Y_{j-1}(x) - \alpha_m Y_j(x)\big). \end{aligned}$$

比较 $Y_0,\cdots,Y_{2m}$ 的系数可得，当 $1\le j\le m$ 时，有

$$y_{2j-1}-\alpha_m y_{2j}+y_{2j+1}=1, \qquad (\mathrm{a})_j$$

$$y_{2j-2}-\alpha_m y_{2j-1}+y_{2j}=a \qquad (\mathrm{b})_j$$

和

$$y_1-(a+\alpha_m)y_0=1, \qquad (\mathrm{c})$$

在此我们已假定 $y_{2m}=y_{2m+1}=0$. 从 $(\mathrm{a})_m$ 可得

$$y_{2m-1}=1=Y_0(\alpha_m).$$

这结合 $(\mathrm{b})_m$ 导出

$$y_{2m-2}=a+\alpha_m=Y_1(\alpha_m).$$

现在归纳地计算

$$y_{2m-(2i+1)} \quad 和 \quad y_{2m-(2i+2)}, \quad i=1,\cdots,[m/2]-1.$$

当 $i=0$ 时，公式显然成立. 现假设公式在 $i-1$ 时成立，即

$$y_{2m-(2i-1)}=Y_0(\alpha_m)+Y_2(\alpha_m)+\cdots+Y_{2i-2}(\alpha_m)$$

和

$$y_{2m-2i}=Y_1(\alpha_m)+Y_3(\alpha_m)+\cdots+Y_{2i-1}(\alpha_m).$$

则从 $(\mathrm{a})_{m-i}$ 和 $(\mathrm{b})_{m-i}$ 分别得到

$$\begin{aligned}y_{2m-2i-1}&=1+\alpha_m y_{2m-2i}-y_{2m-2i+1}\\&=1+\alpha_m\left(Y_1(\alpha_m)+Y_3(\alpha_m)+\cdots+Y_{2i-1}(\alpha_m)\right)\\&\quad-\left(Y_0(\alpha_m)+Y_2(\alpha_m)+\cdots+Y_{2i-2}(\alpha_m)\right)\\&=Y_0(\alpha_m)+Y_2(\alpha_m)+\cdots+Y_{2i}(\alpha_m)\end{aligned}$$

和

$$\begin{aligned}y_{2m-2i-2}&=a+\alpha_m y_{2m-2i-1}-y_{2m-2i}\\&=a+\alpha_m\left(Y_0(\alpha_m)+Y_2(\alpha_m)+\cdots+Y_{2i}(\alpha_m)\right)\end{aligned}$$

$$- (Y_1(\alpha_m) + Y_3(\alpha_m) + \cdots + Y_{2i-1}(\alpha_m))$$
$$= Y_1(\alpha_m) + Y_3(\alpha_m) + \cdots + Y_{2i+1}(\alpha_m),$$

由此即得所需. 为计算剩下的 y_j, 需要按照 m 的奇偶性分两种情况来讨论. 又由于两者的计算是类似的, 故我们只就 m 是偶数的情形加以研究. 对 $i = [m/2] - 1$ 我们有

$$y_{m+1} = Y_0(\alpha_m) + Y_2(\alpha_m) + \cdots + Y_{m-2}(\alpha_m)$$

和

$$y_m = Y_1(\alpha_m) + \cdots + Y_{m-1}(\alpha_m).$$

由于 $Y_m(\alpha_m) = 0$, 故由方程 $(\mathrm{a})_{m/2}$ 和 $(\mathrm{b})_{m/2}$ 可得

$$\begin{aligned} y_{m-1} &= 1 + \alpha_m y_m - y_{m+1} \\ &= 1 + \alpha_m (Y_1(\alpha_m) + \cdots + Y_{m-1}(\alpha_m)) \\ &\quad - (Y_0(\alpha_m) + Y_2(\alpha_m) + \cdots + Y_{m-2}(\alpha_m)) \\ &= Y_0(\alpha_m) + Y_2(\alpha_m) + \cdots + Y_{m-2}(\alpha_m) = y_{m+1} \end{aligned}$$

和

$$\begin{aligned} y_{m-2} &= a + \alpha_m y_{m-1} - y_m \\ &= a + \alpha_m (Y_0(\alpha_m) + Y_2(\alpha_m) + \cdots + Y_{m-2}(\alpha_m)) \\ &\quad - (Y_1(\alpha_m) + \cdots + Y_{m-1}(\alpha_m)) \\ &= Y_1(\alpha_m) + Y_3(\alpha_m) + \cdots + Y_{m-3}(\alpha_m) = y_{m+2}. \end{aligned}$$

同上面一样, 我们可以归纳地证明

$$y_{2m-(2i+1)} = y_{2i+1} \quad 和 \quad y_{2m-(2i+2)} = y_{2i+2}, \quad 0 \le i < [m/2].$$

因此我们就确定了系数 $y_{2m-1}, \cdots, y_1$. 最后, 由 $(\mathrm{b})_1$ 得

$$y_0 = a + \alpha_m y_1 - y_2 = a + \alpha_m Y_0(\alpha_m) - Y_1(\alpha_m) = 0.$$

由于 $y_1 = Y_0(\alpha_m) = 1$, 故上式满足 (c). 命题 4 得证.

定理 13 的证明 可以看出, $Z_m(\alpha_m)=0$, 且当 $x>\alpha_m$ 时 $Z_m(x)>0$, 以及当 $x<\alpha_m$ 时, $Z_m(x)\leq 0$. 对任意的 $\varepsilon>0$, 存在正整数 m,m' 和正常数 z,z', 使得 $\alpha_m,\alpha_{m'}>2-\varepsilon$ 且多项式

$$Z(x)=zZ_m(x)+z'Z_{m'}(x)$$

有下面性质:

(1) $Z(x)=\sum\limits_{i\geq 0}z_iY_i(x)$ 是 $Y_i(x)$ 的非负线性组合;

(2) 当 $x\leq 2-\varepsilon$ 时, $Z(x)\leq -1$;

(3) 当 $x\geq 2$ 时, $Z(x)>0$.

设 Q 是 $Z(x)$ 在区间 $[2-\varepsilon,M]$ 上的最大值. 则 $Q>0$. 设 g',g 分别为区间 $[-M,2-\varepsilon)$ 和 $[2-\varepsilon,M]$ 的特征函数. 由 (6.5) 式知, $\mu_G(Y_i)\geq 0$, 从而有

$$\mu_G(Z)=\sum_i z_i\,\mu_G(Y_i)\geq 0.$$

另一方面,

$$\begin{aligned}\mu_G(Z)&=\mu_G\big(Z(g'+g)\big)=\mu_G(Zg')+\mu_G(Zg)\\&\leq -1\cdot\mu_G(g')+Q\mu_G(g).\end{aligned}$$

由于 $\mu_G(g')=1-\mu_G(g)$, 故从上面两个不等式可得

$$\mu_G(g)\geq\frac{1}{Q+1}.$$

注意 $\mu_G(g)$ 是 G 的所有满足 $\lambda\geq(2-\varepsilon)\sqrt{q}$ 的特征值 λ 所占的比例, 因此我们可取常数 c 为 $1/(Q+1)$, 这是个不依赖于 G 的数. 由此完成了定理 13 的证明.

§7 极限分布

图的**基本闭链**是一条没有折反且不含真子闭链的闭链. 我们用 $c_l(G)$ 表示 G 的长度是 l 的基本闭链的个数. 下面这个 McKay

定理告诉我们，对一族规格增长的正则图，如果其基本闭链的数目是缓增的，则相关于这些图的测度序列收敛于一个好的极限测度.

定理 14[21]　设 $\{G_m\}$ 是一族连通的 k-正则超图，且当 $m \to \infty$ 时，$|G_m| \to \infty$. 假定：

$$\text{对每个 } l \geq 1, \text{ 当 } m \to \infty \text{ 时，有 } c_l(G_m)/|G_m| \to 0. \tag{7.1}$$

则测度序列 $\{\mu_{G_m}\}$ 弱收敛于一个支集是 $[-2,2]$ 的测度

$$\mu = \frac{1+\dfrac{1}{q}}{\left(1+\dfrac{1}{q}-\dfrac{x}{\sqrt{q}}\right)\left(1+\dfrac{1}{q}+\dfrac{x}{\sqrt{q}}\right)} \cdot \frac{1}{\pi}\sqrt{1-\frac{x^2}{4}}\,\mathrm{d}x,$$

其中 $q = k-1$, $\mathrm{d}x$ 是实直线的 Lebesque 测度.

定理 14 给出了一个当 m 很大时图 G_m 的特征值的分布. 特别地，由于任何实数 α 的极限测度是 0, 我们立即可得下面这个在 §8 中将用到的推论.

推论 1　设 $\{G_m\}$ 同定理 14, 它满足条件 (7.1). 则对每个实数 α, α 作为 G_m 的特征值的重数在 $m \to \infty$ 时是 $o(|G_m|)$.

下面的证明取自冯克勤、李文卿的工作 [11], 在那篇文章里，上述结果被推广到了超图. 我们先给出条件 (7.1) 的另一种解释.

命题 5　条件 (7.1) 等价于

$$\text{对每个整数 } l \geq 1, \ \mathrm{Tr}\,U_l(G_m)/|G_m| \text{ 在 } m \to \infty \text{ 时趋于0.} \tag{7.2}$$

证　由于图 G 的每个长度为 l 的基本闭链对 $\mathrm{Tr}\,U_l(G)$ 的贡献是 1, 所以

$$\mathrm{Tr}\,U_l(G) \geq c_l(G).$$

因此由 (7.2) 可导出 (7.1). 反过来，假定 (7.1) 成立. 由于 G 中一条没有折反、长度为 l 且对 $\mathrm{Tr}\,U_l(G)$ 没有贡献的路径一定是 G 的一条闭链，于是它至少包含一条 G 中长度 $j \leq l$ 的基本闭链. 又因这样一条基本闭链至多含于 $(l-j+1)q^{l-j}$ 条 G 的长度为 l 且不

折反的闭链中，于是在 G 中至多有

$$\sum_{j=1}^{l}(l-j+1)q^{l-j}c_j(G)$$

个长度为 l 的闭链．从而就证明了

$$\operatorname{Tr}U_l(G) \leq \sum_{j=1}^{l}(l-j+1)q^{l-j}c_j(G).$$

由此容易看出，从 (7.1) 可导出 (7.2).

我们将在条件 (7.2) 成立的前提下证明定理 14．以 μ_m 代表 μ_{G_m}．由上节的分析可知，要证明 μ_m 的极限存在，我们必须证明极限 $\lim\limits_{m\to\infty}\mu_m(Y_l)$ 对每个 $l \geq 0$ 存在．从 (6.4) 和 (6.2) 式给出的 T_l 的定义看到，当 $l \geq 1$ 时，

$$q^{l/2}\mu_m(Y_l) - q^{(l-1)/2}\mu_m(Y_{l-1}) = \frac{1}{|G_m|}\operatorname{Tr}U_l(G_m).$$

因此由条件 (7.2) 导出，对每个 $l \geq 1$,

$$\lim_{m\to\infty} q^{l/2}\mu_m(Y_l) - q^{(l-1)/2}\mu_m(Y_{l-1}) = 0.$$

结合 $\mu_m(Y_0) = 1$，上述讨论导出 $\lim\limits_{m\to\infty}\mu_m(Y_l)$ 存在且在 $l \geq 0$ 时等于 $q^{-l/2}$．换句话说，即极限 $\lim\limits_{m\to\infty}\mu_m$ 存在，记此极限为 μ．则对 $l \geq 0$ 有 $\mu(Y_l) = q^{-l/2}$．将 μ 与 §6 中 (III) 给出的 Sato-Tate 测度 ρ 进行比较可知，我们现在必需算出 $\mu(X_l)$．从 Y_l 的定义可以归纳地得出，当 $l \geq 0$ 时，

$$X_l = Y_l - aY_{l-1} + a^2Y_{l-2} - a^3Y_{l-3} + \cdots + (-a)^lY_0,$$

其中 $a = 1/\sqrt{q}$．因此

$$\begin{aligned}\mu(X_l) &= \sum_{i=0}^{l}(-a)^i\mu(Y_{l-i}) = \sum_{i=0}^{l}(-1)^iq^{-\frac{l}{2}}\\ &= \frac{1}{2}\left(q^{-\frac{l}{2}} + (-1)^lq^{-\frac{l}{2}}\right).\end{aligned}$$

从而利用 §6 中 (I) 得

$$\sum_{l=0}^{\infty}\mu(X_l)X_l(x)=\sum_{l=0}^{\infty}\frac{1}{2}X_l(x)q^{-\frac{l}{2}}+\frac{1}{2}\sum_{l=0}^{\infty}X_l(x)(-1)^l q^{-\frac{l}{2}}$$
$$=\frac{1}{2}\frac{1}{1-xq^{-1/2}+q^{-1}}+\frac{1}{2}\frac{1}{1+xq^{-1/2}+q^{-1}}$$
$$=\left(1+\frac{1}{q}\right)\Big/\left(1+\frac{1}{q}-\frac{x}{\sqrt{q}}\right)\left(1+\frac{1}{q}+\frac{x}{\sqrt{q}}\right).$$

因此 μ 就是所需的极限测度. 定理 14 得证.

§8 在 p 处具有整特征值的尖点形式空间维数大小的估计

固定一个素数 p. 对一个与 p 互素的正整数 N, 用 $C'(\Gamma_0(N),2)$ 表示由这样的一些 $\Gamma_0(N)$ 的权为 2 的尖点形式生成的空间, 它们是 Hecke 算子 $\mathbb{T}_p$ 的具有整特征值的特征函数. 在这一节里, 我们将利用上一节的结果给出空间 $C'(\Gamma_0(N),2)$ 维数的增长的一个估计. 这一结果出自参考文献 [11]. 在此, 我们将介绍下面这个更精细的描述.

定理 15 (1)[29] 设 $\{l_i\}$ 是一个由异于 p 的素数组成的序列, 且在 $i\to\infty$ 时, $l_i\to\infty$. 则对充分大的 i 有

$$\dim C'(\Gamma_0(l_i),2)=o(l_i).$$

(2)[11] 设 $\{M_i\}$ 是一个由与 p 互素的整数组成的序列, 且

$$M_i=l_iN_i,$$

其中 l_i 是一个不整除 N_i 的素数, 并且满足当 $i\to\infty$ 时, $l_i\to\infty$. 那么对充分大的 i, 若 M_i 的素因子的个数是有界的, 则

$$\dim C'(\Gamma_0(M_i),2)=o(M_i);$$

否则

$$\dim C'\big(\Gamma_0(M_i),2\big) = o(M_i \ln\ln M_i).$$

注意，在 (2) 中，我们可选择 M_i 是无平方因子的，l_i 是 M_i 的最大素因子．于是当 $M_i \to \infty$ 时，l_i 也趋于 ∞.

我们将在一类特殊的由四元数代数构造的图上应用定理 14. 给定素数 p. 对一个素数 $l \neq p$, 记 H_l 为 $\mathbf{Q}$ 上在 ∞ 和 l 处分歧的四元数代数．用 D_l 表示 $H_l^\times$ 的乘法群关于其中心的商群．对 D_l 中的阿代尔点有强逼近定理成立：

$$D_l(A_{\mathbf{Q}}) = D_l(\mathbf{Q})\cdot D_l(\mathbf{R})D_l(\mathbf{Q}_p)K,$$

其中 $K = \prod\limits_{q\neq p,\infty} K_q$ 是限制直积 $\prod\limits_{q\neq p,\infty} D_l(\mathbf{Q}_q)$ 的一个紧开子群，且使得 K 在简约范数映射下的像是所有 $\mathbf{Q}_q$ 的单位根群的积，这里 q 过所有 $\neq p$ 的 $\mathbf{Q}$ 的有限位．在使 H_l 分歧的位 l 处，取 K_l 是 $D_l(\mathbf{Q}_l)$ 的最大紧子群；在一个异于 l,p 和 ∞ 的位 q 处，H_l 是分裂的，从而 $D_l(\mathbf{Q}_q)$ 同构于 $\mathrm{PGL}_2(\mathbf{Q}_q)$, 我们取

$$K_q = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathbf{Z}_q) : \mathrm{ord}_q c \geq n(q) \right\} \Big/ \left\{ \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \in \mathrm{GL}_2(\mathbf{Z}_q) : \mathrm{ord}_q a = 0 \right\},$$

使得对所有的 $q \neq l,p,\infty$, 有 $n(q) \geq 0$, 其中，对几乎所有的 q, 都有 $n(q) = 0$. 设

$$N = \prod_{q\neq l,p,\infty} q^{n(q)},$$

且记这样选取的群 K 为 $B_0(l,N)$. 交集

$$D_l(\mathbf{Q}) \bigcap D_l(\mathbf{R})D_l(\mathbf{Q}_p)B_0(l,N)$$

是 $D_l\left(\mathbf{Z}\left[\frac{1}{p}\right]\right)$ 的一个同余子群，我们记作 $\widetilde{\Gamma_0}(l,N)$. 利用强逼近定

理知，双边陪集空间

$$X(l,N)=D_l(\mathbf{Q})\backslash D_l(A_{\mathbf{Q}})/D_l(\mathbf{R})B_0(l,N)D_l(\mathbf{Z}_p)$$

亦可由在位 p 处的双边陪集空间来表示：

$$\begin{aligned}X(l,N)&=\widetilde{\Gamma_0}(l,N)\backslash D_l(\mathbf{Q}_p)/D_l(\mathbf{Z}_p)\\&=\widetilde{\Gamma_0}(l,N)\backslash \mathrm{PGL}_2(\mathbf{Q}_p)/\mathrm{PGL}_2(\mathbf{Z}_p).\end{aligned}$$

按 §3 的解释，$\mathrm{PGL}_2(\mathbf{Q}_p)/\mathrm{PGL}_2(\mathbf{Z}_p)$ 有一个自然的结构作为 $(p+1)$-正则无限树 $\mathcal{T}$，且当它是无挠时，$\widetilde{\Gamma_0}(l,N)$ 作为 $\mathrm{PGL}_2(\mathbf{Q}_p)$ 的一个离散子群是图 $X(l,N)=\widetilde{\Gamma_0}(l,N)\backslash\mathcal{T}$ 的基本群．由于 H_l 在 ∞ 处分歧，所以此图是有限的，且在计入可能的回路及重边后，它还是 $(p+1)$-正则的．$X(l,N)$ 的邻接矩阵恰好是作用在 $D_l(A_{\mathbf{Q}})$ 上的自守形式空间上的 Hecke 算子 $\mathbb{T}_p$，这些自守形式要求在 $D_l(\mathbf{Q})$ 左作用下不变，且在 $D_l(\mathbf{R})B_0(l,N)D_l(\mathbf{Z}_p)$ 的右作用下亦不变．

当 l 趋于无穷时，我们将对图族 $\{X(l,N)\}$ 给出一个类似于推论 1 的结论．为此，我们需要验证 §7 命题 5 中的条件 (7.1) 或等价条件 (7.2)．

命题 6[29] *对任意的 $n\geq 1$，存在一个仅依赖于 p^n 而不依赖于 l 的常数 $C(n,p)$，使得*

$$0\leq \mathrm{Tr}\,U_n\big(X(l,1)\big)\leq C(n,p).$$

证 图 $X(l,1)$ 的顶点可以被看做是特征 l 的超奇异椭圆曲线的等价类，两个这样的类相邻的充分必要条件是它们可被 p 次同源的两条椭圆曲线代表．因此 U_n 在 $X(l,1)$ 上的迹基本上就等于以一个 p^n 阶的循环群为核的自同源的椭圆曲线类的个数．我们已经知道这样的类有一个独立于 l 的界．这就证明了命题 6．

因此，当 $n\geq 1$ 时，图 $X(l,1)$ 中长度为 n 且不折反的闭链数目不超过 $C(n,p)$，且它与 l 无关．现在我们来研究 $X(l,N)$ 中这样闭链的数目．注意 $X(l,N)$ 是 $X(l,1)$ 的一个次数为 $\left[\widetilde{\Gamma_0}(l,1):\widetilde{\Gamma_0}(l,N)\right]$ 的覆盖图．$X(l,N)$ 中的每个长度皆为 n 且不折反的闭链的投影为

$X(l,1)$ 中具有相同性质的闭链. 因此

$$\operatorname{Tr} U_n\big(X(l,N)\big) \le \big[\widetilde{\Gamma_0}(l,1) : \widetilde{\Gamma_0}(l,N)\big] \operatorname{Tr} U_n\big(X(l,1)\big).$$

从而

$$0 \le \frac{\operatorname{Tr} U_n\big(X(l,N)\big)}{|X(l,N)|} \le \frac{\big[\widetilde{\Gamma_0}(l,1) : \widetilde{\Gamma_0}(l,N)\big] \operatorname{Tr} U_n\big(X(l,1)\big)}{\big[\widetilde{\Gamma_0}(l,1) : \widetilde{\Gamma_0}(l,N)\big] |X(l,1)|}$$

$$= \frac{\operatorname{Tr} U_n\big(X(l,1)\big)}{|X(l,1)|} \le \frac{C(n,p)}{|X(l,1)|}.$$

我们看到上界的分子是独立于 l 和 N 的, 而分母则在 l 趋于 ∞ 时趋于 ∞. 这就证明了下面的命题 7.

命题 7 给出一个素数序列 $\{l_i\}$, 其中 $l_i \neq p$, 且当 $i \to \infty$ 时 $l_i \to \infty$. 又给出一个正整数序列 $\{N_i\}$, 其中 N_i 与 pl_i 互素. 则对任意的 $n \ge 1$, 当 $i \to \infty$ 时, 我们有

$$\frac{c_n\big(X(l_i,N_i)\big)}{|X(l_i,N_i)|} \longrightarrow 0.$$

因此推论 1 对图族 $\{X(l_i,N_i)\}$ 成立. 更精确些, 我们有

命题 8 设 $\{l_i\}$ 和 $\{N_i\}$ 同定理 15. $\mathcal{A}\big(\widetilde{\Gamma_0}(l_i,N_i)\big)$ 是

$$D_{l_i}(\mathbf{Q})\backslash D_{l_i}(A_{\mathbf{Q}})/D_{l_i}(\mathbf{R})D_{l_i}(\mathbf{Z}_p)B(l_i,N_i)$$

上的自守形式空间. 对任意给出的实数 α, α 作为 $\mathcal{A}\big(\widetilde{\Gamma_0}(l_i,N_i)\big)$ 上 Hecke 算子 $\mathbb{T}_p$ 的特征值满足: 当 $i \to \infty$ 时, α 的重数为 $o\big(|X(l_i,N_i)|\big)$.

接下来, 我们分析自守形式空间 $\mathcal{A}\big(\widetilde{\Gamma_0}(l_i,N_i)\big)$. 首先, 它包含常值函数, 而这是 $\mathbb{T}_p$ 的特征值为 $p+1$ 的特征函数. 用 $\mathcal{A}^{\perp}\big(\widetilde{\Gamma_0}(l_i,N_i)\big)$ 表示 $\mathcal{A}\big(\widetilde{\Gamma_0}(l_i,N_i)\big)$ 中垂直于常值函数的函数全体组成的空间, 它显然是 $\mathbb{T}_p$-不变的, 且其余维数是 1. 进一步, 利用由 Jacquet 和 Langlands 建立的 GL_2 和四元数群上的自守形式理论以及由 Gelbart 和 Jacquet 给出的对应 (参阅第八章), 空间 $\mathcal{A}^{\perp}\big(\widetilde{\Gamma_0}(l_i,N_i)\big)$ 中的自守形式等同于由 $\Gamma_0(l_iN_i)$ 上权 2 的尖点形式生成的空间 $C_{l_i}\big(\Gamma_0(l_iN_i),2\big)$ 中的自守形式. 出现于该空间中的 $\mathrm{GL}_2(A_{\mathbf{Q}})$ 的自守表示在 l_i 处有

一个是 $\mathrm{GL}_2(\mathbf{Q}_{l_i})$ 的非分歧的特殊表示的连通分支. 于是, $\mathbb{T}_p$ 在 $\mathcal{A}^{\perp}(\widetilde{\Gamma_0}(l_i,N_i))$ 上的特征值恰好是那些 $\mathbb{T}_p$ 在 $\Gamma_0(l_iN_i)$ 上的权 2 的尖点形式空间 $\mathcal{C}(\Gamma_0(l_iN_i),2)$ 上的特征值. 利用我们在第七章讨论的 Ramanujan-Petersson 猜想知, $\mathbb{T}_p$ 在权 2 的尖点形式上的特征值 λ_p 满足

$$|\lambda_p| \le 2\sqrt{p}.$$

于是, $\mathbb{T}_p$ 在 $\mathcal{A}^{\perp}(\widetilde{\Gamma_0}(l_i,N_i))$ 中只可能有有限多个整的特征值. 结合命题 8, 这就证明了:

定理 16 设 $\{l_i\}$ 是一个由 $\ne p$ 的素数组成的序列, 且当 $i\to\infty$ 时, $l_i\to\infty$. 设 $\{N_i\}$ 是一个正整数序列, 且 N_i 与 pl_i 互素. 则当 $i\to\infty$ 时, 由在空间 $\mathcal{A}^{\perp}(\widetilde{\Gamma_0}(l_i,N_i))$ 中 $\mathbb{T}_p$ 的具有整特征值的特征函数生成的空间 $\mathcal{A}'(\widetilde{\Gamma_0}(l_i,N_i))$ 的维数为 $o(|X(l_i,N_i)|)$.

关于集合 $X(l_i,N_i)$ 的大小, 我们有

$$\begin{aligned}|X(l_i,N_i)| &= \dim \mathcal{A}(\widetilde{\Gamma_0}(l_i,N_i)) = 1+\ \dim \mathcal{A}^{\perp}(\widetilde{\Gamma_0}(l_i,N_i))\\ &\le 1+\ \dim \mathcal{C}(\Gamma_0(l_iN_i),2).\end{aligned}$$

另一方面, $\dim\mathcal{C}(\Gamma_0(l_iN_i),2)$ 是模群 $\Gamma_0(l_iN_i)$ 的亏格, 其主项是

$$\frac{1}{12}\, l_iN_i \prod_{\substack{q|l_iN_i\\ q\text{素数}}} \left(1+\frac{1}{q}\right)$$

(参见参考文献 [25]). 于是当 $i\to\infty$ 时,

$$|X(l_i,N_i)| = O\left(l_iN_i\prod_{q|l_iN_i}\left(1+\frac{1}{q}\right)\right).$$

我们对几种特殊情形来应用定理 16, 从而给出定理 15 的证明. 首先考虑对所有的 i, $N_i=1$ 的情况. 由于没有权 2 的 $\mathrm{SL}_2(\mathbf{Z})$ 的尖点形式, 所以

$$\mathcal{C}_{l_i}(\Gamma_0(l_iN_i),2) = \mathcal{C}(\Gamma_0(l_i),2).$$

于是定理 15 的第一个结论立即可从定理 16 得出. 接下来讨论 $M = lN$ 这种情形, 其中 l 与 N 互素. 此时利用第七章 §3 研究的新形式理论知, $\mathcal{C}_l(\Gamma_0(M),2)$ 在 $\mathcal{C}(\Gamma_0(M),2)$ 中的正交补是 $\mathbb{T}_p$-不变的, 并且它可由 $\mathcal{C}(\Gamma_0(N),2)$ 和它在 l 处的"提升"生成, 从而有

$$\dim \mathcal{C}(\Gamma_0(M),2) = \dim \mathcal{C}_l(\Gamma_0(M),2) + 2\dim \mathcal{C}(\Gamma_0(N),2).$$

我们用加撇"$'$"的方式来表示自守形式空间中由那些是 $\mathbb{T}_p$ 的具有整特征值的特征函数生成的子空间. 由于在 l 处的提升算子与 $\mathbb{T}_p$ 可交换, 所以由上面公式可得

$$\begin{aligned}\dim \mathcal{C}'(\Gamma_0(M),2) &= \dim \mathcal{C}_l'(\Gamma_0(M),2) + 2\dim \mathcal{C}'(\Gamma_0(N),2)\\ &= \dim \mathcal{A}'(\widetilde{\Gamma_0}(l,N)) + 2\dim \mathcal{C}'(\Gamma_0(N),2).\end{aligned}$$

借助上面的讨论可得

$$\dim \mathcal{C}'(\Gamma_0(N),2) \le \dim \mathcal{C}(\Gamma_0(N),2) \ll N\prod_{q|N}\left(1+\frac{1}{q}\right).$$

于是

$$2\dim \mathcal{C}'(\Gamma_0(N),2) \ll M\prod_{q|M}\left(1+\frac{1}{q}\right)\cdot\frac{2}{l+1}.$$

现在命 $M = M_i = l_iN_i$, 其中当 $i\to\infty$ 时, $l_i\to\infty$. 由定理 16 知

$$\dim \mathcal{A}'(\widetilde{\Gamma_0}(l_i,N_i)) = o\left(M_i\prod_{q|M_i}\left(1+\frac{1}{q}\right)\right).$$

从上面的分析可看出, 对 $2\dim \mathcal{C}'(\Gamma_0(N_i),2)$ 也有同样的的估计. 于是, 当 $i\to\infty$ 时有

$$\dim \mathcal{C}'(\Gamma_0(M_i),2) = o\left(M_i\prod_{q|M_i}\left(1+\frac{1}{q}\right)\right).$$

若全体 M_i 的素因子数目有界, 则

$$\prod_{q|M_i}\left(1+\frac{1}{q}\right)$$

是有界的；否则，

$$\prod_{q|M_i}\left(1+\frac{1}{q}\right)$$

是 $O(\ln\ln M_i)$(参见参考文献 [13] 第 90 页)．这就证明了定理 15 的第二个结论．由此定理 15 完全得证．

作为我们证明的一个副产品，结合命题 7 和定理 14 可得：

定理 17 设 $\{l_i\}$ 是一个由不等于 p 的素数组成的序列，且当 $i\to\infty$ 时，$l_i\to\infty$．设 $\{N_i\}$ 是一个正整数序列，且 N_i 与 pl_i 互素．则当 $i\to\infty$ 时，Hecke 算子 $\mathbb{T}_p$ 在 $\Gamma_0(l_iN_i)$ 上权为 2 的尖点形式空间中的特征值 (通过除以 $2\sqrt{p}$ 来正规化) 关于下面这个测度 μ 是一致分布的．μ 的支集是 $[-2,2]$，在支集上的定义为

$$\mu=\frac{1+\dfrac{1}{p}}{\left(1+\dfrac{1}{p}-\dfrac{x}{\sqrt{p}}\right)\left(1+\dfrac{1}{p}+\dfrac{x}{\sqrt{p}}\right)}\cdot\frac{1}{\pi}\sqrt{1-\frac{x^2}{4}}\,\mathrm{d}x,$$

其中 $\mathrm{d}x$ 是实直线上的 Lebesque 测度．特别地，当素数 $l\to\infty$ 时，Hecke 算子 $\mathbb{T}_p$ 在权为 2，水平为 l 的尖点形式空间上的正规化特征值关于 μ 是一致分布的．

参 考 文 献

[1] N. Alon and V. Milman, λ_1, *isoperimetric inequalities for graphs and superconcentrators*, J. Comb. Theory Ser.B, **38** (1985), 73~88.

[2] J. Angel, N. Celniker, S. Poulos, A. Terras, C. Trimble, and E. Velasquez, *Special functions on finite upper half planes*, Contemp. Math., **138** (1992), 1~26.

[3] F. Bien, *Constructions of telephone networks by group representations*, Notices of Amer. Math. Soc., **36** (1989), 5~22.

[4] R. Brooks, *The spectral geometry of a tower of coverings*, J. Diff. Geom., **23** (1986), 97~107.

[5] N. Celniker, S. Poulos, A. Terras, C. Trimble, and E. Velasquez, *Is there life on finite upper half planes?* Contemp. Math., **143** (1993), 65~88.

[6] J. Cheeger, *A lower bound for the smallest eigenvalue of the Laplace operator*, Problems in Analysis, Gunning ed., Princeton Univ. Press, 1970, 195~199.

[7] P. Chiu, *Cubic Ramanujan graphs*, Combinatorica, **12**(1992), 275~285.

[8] F. R. K. Chung, *Diameters and eigenvalues*, J. Amer. Math. Soc., **2** (1989), 187~196.

[9] V. G. Drinfeld, *The proof of Petersson's conjecture for $GL(2)$ over a global field of characteristic p*, Functional Anal. Appl., **22** (1988), 28~43.

[10] R. Evans, *Character sums as orthogonal eigenfunctions of adjacency operators for Cayley graphs*, preprint, 1993.

[11] 冯克勤 (K. Feng) and 李文卿 (W.-C. W. Li), Spectra of hypergraphs and applications, J. Number Theory (待发表).

[12] O. Gabber and Z. Galil, *Explicit construction of linear sized superconcentrators*, J. Comput. Sys. Sci., **22** (1981), 407~420.

[13] 华罗庚, 《数论导引》, 科学出版社, 北京, 1958.

[14] N. Katz, *Estimates for Soto-Andrade sums*, J. reine angew. Math., **438** (1993), 143~161.

[15] 李文卿 (W.-C. W. Li), *Character sums and abelian Ramanujan graphs*, J. Number Theory, **41** (1992), 199~217.

[16] 李文卿 (W.-C. W. Li), *Number theoretic constructions of Ramanujan graphs*, Astérisque, Soc. Math. de French, **228** (1995), 101~120.

[17] 李文卿 (W.-C. W. Li), *A survey of Ramanujan graphs*, In: Arithmetic Geometry and Coding Theory, Proceedings of International Confrerence held at Luminy, France, June 28~July 2, 1993, de Gruyter Proc., 1996.

[18] A. Lubotzky, R. Phillips and P. Sarnak, *Ramanujan graphs*, Combi-

natorica, **8** (1988), 261~277.

[19] G. Margulism, *Explicit construction of concentrators*, Problems of Information Transmission, **9** (1975), 325-332.

[20] G. Margulis, *Explicit group theoretic constructions of combinatorial schemes and their application to the design of expanders and concentrators*, J. Prob. of Info. Trans., 1988, 39~46.

[21] B. D. McKay, *The expected eigenvalue distribution of a large regular graph*, Linear Alg. and Its Appli., **40** (1981), 203~216.

[22] J.-F. Mestre, *La méthode des graphes. Exemples et applications*, Proc. Int. Conf. on Class Numbers and Fundamental Units of Algebraic Number Fields, June 24~28, 1986, Katata, Japan, 217~242.

[23] M. Morgenstern, *Existence and explicit constructions of $q+1$ regular Ramanujan graphs for every prime power q*, J. Comb. Theory, series B **62** (1994). 44~62.

[24] A. Nilli, *On the second eigenvalue of a graph*, Disc. Math., **91** (1991), 207~210.

[25] A. P. Ogg, *Modular Forms and Dirichlet Series*, Benjamin, New York, 1969.

[26] I. I. Piatetski-Shapiro, *Complex Representations of* $\mathrm{GL}(2, K)$ *for Finite Field K*, Contemporary Math. 16, Amer. Math. Soc., Providence, 1983.

[27] A. Pizer, *Ramanujan graphs and Hecke operators*, Bull. Amer. Math. Soc., **23** (1990), 127~137.

[28] J.-P. Serre, *Trees*, Springer-Verlag, Berlin, Heidelberg, New York, 1980.

[29] J.-P. Serre, *Private letter to W.-C. W. Li*, dated Oct. 8, 1990 and Nov. 5, 1990.

[30] J. Soto-Andrade, *Geometrical Gel'fand models, tensor quotients and Weil representations*, Proc. Symp. Pure Math. 47, Amer. Math. Soc., Providence (1987), 305~316.

[31] T. Sunada, *L^2-functions in geometry and some applications*, Proc. Taniguchi Symp. 1985, Lecture Notes in Math. 1201, Springer-Verlag, Berlin, Heidelberg, New York (1986), 266~284.

[32] T. Sunada, *Fundamental groups and Laplace operators*, Lecture Notes in Math. 1339, Springer-Verlag, Berlin, Heidelberg, New York (1988), 248~277.

[33] R. Tanner, *Explicit concentrators from generalized N-gons*, SIAM J. Alg. Dis. Math., **5** (1984), 287~293.

[34] A. Weil, *On some exponential sums*, Proc. Nat. Aca. Sci., **34** (1948), 204~207.

索　引

[General Information]
书名=数论及其应用
作者=李文卿著
页数=372
SS号=11052107
DX号=
出版日期=2001年03月第1版
出版社=北京大学出版社